PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-022216
(43)Date of publication of application : 24.01.2003

(51)Int.Cl. G06F 12/14
B42D 15/10
G06K 19/07

(21)Application number : 2001-207210
(22)Date of filing : 09.07.2001

(71)Applicant : HITACHI LTD
(72)Inventor : HATANO TOMIHISA
TODA AKINORI
TSUNODA MOTOYASU
MIZUSHIMA EIGA
KATAYAMA KUNIHIRO

(54) STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize the high speed processing of a multi-media card.
SOLUTION: This storage device is provided with a flash memory chip 130, an IC card chip 150 capable of executing security processing (encryption or decoding or the like), and a controller chip 120 for controlling the reading/ writing of data for the flash memory chip and the IC card chip. Moreover, the controller chip 120 simultaneously accesses the flash memory chip 130 and the IC chard chip 150 in response to a request from a host.

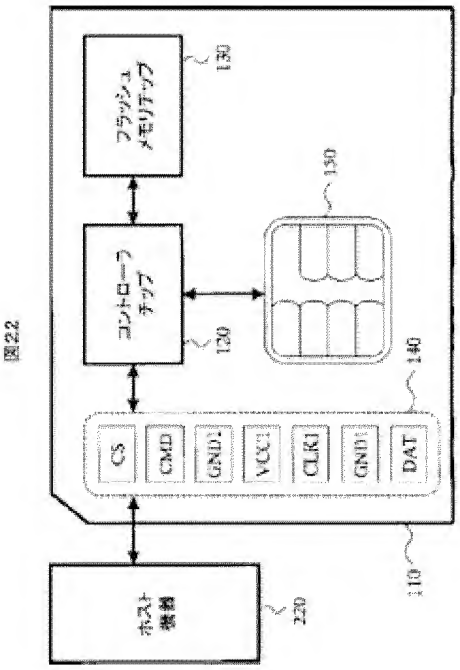


図22

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]In memory storage for memorizing, data The 1st memory that can memorize said data, The 2nd memory in which said data is memorizable and that can perform security processing of said data, Based on a command from host equipment, it has a controller which chooses said 1st memory or said 2nd memory, Memory storage performing processing which receives the 2nd command from said host equipment to said 2nd memory while performing access to said 1st memory from said host equipment, and follows said 2nd command.
[Claim 2]The memory storage according to claim 1 with which said controller chooses said 2nd memory when information about security processing of said data is included in a command from said host equipment.
[Claim 3]The memory storage according to claim 1, wherein said 2nd memory is the IC chip beforehand attested by security evaluator Seki.
[Claim 4]The memory storage according to claim 3, wherein said attested IC chip has a means to encipher or decrypt data written to this attested IC chip.
[Claim 5]The 1st storage area where said 1st memory memorizes data from said host equipment, The memory storage according to claim 4 having the 2nd storage area that memorizes data about said 2nd memory, and where at least one of read-out of data from said host equipment or the writing is restricted.
[Claim 6]The memory storage according to claim 5, wherein said controller has a means to transmit data memorized in said 2nd storage area to said 2nd memory.
[Claim 7]The memory storage according to claim 6, wherein said controller controls said 2nd memory based on data memorized in said 2nd storage area.
[Claim 8]A memory which memorizes the first and the second contents which were enciphered by a session key published by content provider, An arithmetic processing unit with a memory which a session key enciphered by said content provider by a public key and a secret key corresponding to said public key are memorized, and can decrypt said session key with said secret key, While said session key corresponding to said first contents makes said arithmetic processing unit with a memory decrypt according to a command from a host, Memory storage provided with a controller which decrypts said second contents memorized by said memory with said session key corresponding to said second already decrypted contents, and transmits said decrypted contents to said host.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]The memory storage with which this invention carried the security function, the host equipment which can insert the memory storage, And the host equipment in which the memory storage was inserted is started, and it is related with the terminal unit with which the device which can insert the memory card which has a flash memory chip and a controller especially, and its memory card, and its memory card of its were inserted.
[0002]
[Description of the Prior Art]An IC card embeds IC (integrated circuit) chip into a plastic card board, and has an external terminal of an IC chip in the surface. A power supply terminal, a clock terminal, a data input/output terminal, etc. are contained in the external terminal of an IC chip. The IC chip operates, when a contact carries out direct supply of a power supply or the driving clock from an external terminal.
[0003]An IC card exchanges information with a contact by transmitting and receiving an electrical signal among contacts, such as a terminal, through an external terminal. As a result of information exchange, an IC card performs sending out of a calculation result or memory information, and change of memory information. The IC card can have the function to perform security processings, such as security data protection and personal authentication, based on such operation specifications. In the system for which the security of extra sensitive information, such as credit settlement and banking, is needed, the IC card is used as a user device for identification.
[0004]
[Problem(s) to be Solved by the Invention]The IC card used in a security system needs to be designed not leak the information which can presume the confidential information or its confidential information to the exterior of an IC card when calculating using confidential information inside an IC card. That is, to have the Tampa-proof nature is needed. As the attack method of analyzing the confidential information which must not be leaked to such the exterior, a timing analysis, power difference part analysis, failure use analysis, etc. are known.
[0005]A timing analysis is the attacking method for analyzing the time lag statistically and presuming confidential information, when cipher-processing time differs depending on the contents of confidential information. When a cryptographic algorithm is mounted in a device, optimization which skips the processing which becomes unnecessary depending on the contents of confidential information for the purpose of shortening of the processing time of a code or reduction of program size, or performs a branching process may be performed. When such optimization is performed, cipher-processing time differs depending on the contents of confidential information. Therefore, the contents of confidential information may be able to be presumed by seeing processing time.
[0006]While power difference part analysis is performing cipher processing, it is the attacking method for presuming confidential information by measuring the electric power supplied from the power supply terminal of an IC card, and analyzing the difference of power consumption from there.
[0007]Failure use analysis is the attacking method using the miscalculation of the IC card. A restrictive obstacle of the range of not affecting transient failure or other functions is done to an IC card, and the unusual processing which an aggressor expects to an IC card is made to perform. For example, confidential information may be acquired from the mistaken calculation result obtained when an error is intentionally generated by applying high tension to an IC card, or fluctuating a clock frequency and driver voltage momentarily, and a right calculation result.
[0008]Therefore, the IC card must have a measure means against these attacking methods practically.

[0009]The purpose of this invention is to provide the memory storage which improved security.
[0010]
[Means for Solving the Problem]In memory storage for this invention to memorize data in order to solve an aforementioned problem, The 2nd memory [remember / and / to be the 1st memory that can memorize data / data] that can perform security processing of data, Based on a command from host equipment, it has with a controller which chooses the 1st memory or 2nd memory, While performing access to the 1st memory from host equipment, the 2nd command from a host to the 2nd memory is received, and it has composition which performs processing according to the 2nd command.
[0011]When information about security processing of data is included in a command from host equipment, composition which chooses the 2nd memory may be sufficient as a controller.
[0012]It is also considered that the 2nd memory is the IC chip beforehand attested by security evaluator Seki.
[0013]An attested IC chip has a means to encipher or decrypt data written to an attested IC chip.
[0014]The 1st memory can memorize data about the 1st storage area that memorizes data from host equipment, and the 2nd memory, and can also consider it as composition which has the 2nd storage area where at least one of read-out of data from host equipment or the writing is restricted.
[0015]The controller can also have a means to transmit data memorized in the 2nd storage area to the 2nd memory.
[0016]A controller may have the composition which controls the 2nd memory based on data memorized in the 2nd storage area.
[0017]A memory which memorizes the first and the second contents which were enciphered by a session key published by content provider as an embodiment of this invention, An arithmetic processing unit with a memory which a session key enciphered by content provider by a public key and a secret key corresponding to a public key are memorized, and can decrypt a session key with a secret key, While a session key corresponding to the first contents makes an arithmetic processing unit with a memory decrypt according to a command from host equipment, It has composition which has a controller which decrypts the second contents memorized by memory with a session key corresponding to the second already decrypted contents, and transmits the second decrypted contents to host equipment.
[0018]
[Embodiment of the Invention]MultiMediaCard to which drawing 22 applied this invention (MultiMediaCard is a registered trademark of InfineonTechnologiesAG.) Hereafter, it is written as "MMC". It is a figure showing an internal configuration. As for MMC110, being based on MMC specification is preferred. MMC110 has the security processing function to perform a code operation required for security data protection, personal authentication, etc., based on the memory card command based on the MMC specification published from the host equipment 220 connected to MMC110.
[0019]As for the host equipment 220, a cellular phone, a Personal Digital Assistant (PDA), a personal computer, a music reproduction (and sound recording) device, a camera, a video camera, automatic deposit ******, a street corner terminal, a settlement system, etc. correspond, for example.
[0020]MMC110 has the MMC external terminal 140, the controller chip 120, the flash memory chip 130, and the IC card chip 150. The flash memory chip 130 is a memory chip which uses nonvolatile semiconductor memory as a storage, and can perform reading and writing of data with a flash plate memory command. The MMC external terminal 140 comprises seven terminals, such as a power supply terminal, a clock input terminal, a command input/output terminal, a data input/output terminal, and a ground terminal, in order to exchange information with the external host equipment 220. The controller chip 120 is a microcomputer chip which is connected with the MMC external terminal 140, the flash memory chip 130, and the IC card chip 150, and controls these.
[0021]The IC card chip 150 is a microcomputer chip for embedding into the plastic plate of an IC card, and the external terminal, electrical signal protocol, and command which the IC card chip 150 has are based on ISO/IEC7816 standard. There are a power supply terminal, a clock input terminal, a reset input terminal, an I/O input/output terminal, and a ground terminal in the external terminal of the IC card chip 150. The controller chip 120 performs an operation required for the security processing demanded from the external host equipment 220 by publishing an IC card command from the external terminal of the IC card chip 150 to the IC card chip 150.
[0022]Drawing 26 is a figure showing the internal configuration of IC card chip of this invention. The IC card chip 150, Data processing. CPU(microcomputer) 158 for carrying out, data (a program.) it

contains. ROM (ReadOnly.) for memorizing The processing carried out to Memory159, RAM(Random Access Memory) 160, EEPROM(Electrically Erasable ProgrammableROM) 162, and a code/decoding in between. It has the serial interface 161 for transmitting and receiving the code co-processor 163, and the exterior and data for carrying out. These are mutually connected by bus 164.

[0023]The code co-processor 163 performs security processing according to the command from the host equipment 220. Instead of the code co-processor 163 (hardware), a program (software) may be used and CPU158 may perform security processing. Security processing is performed, for example, when data is written in the storage area in the IC card chip 150, or when data is read from the storage area in the IC card chip 150.

[0024]The flash memory chip 130 has a nonvolatile storage cell. Generally, the storage capacity of EEPROM162 of the IC card chip 150 is smaller than the storage capacity of the flash memory chip 130. However, the storage capacity of EEPROM162 may be the same as that of the flash memory chip 130, and may be large.

[0025]It is desirable to use for the IC card chip 150 the product which is ending with attestation by evaluation and the certificate authority of ISO/IEC15408 which is international standards of a security valuation basis. When using the IC card which generally has the function to perform security processing by a actual electronic payment service etc., the IC card needs to receive the evaluation and authorization by evaluation and a certificate authority of ISO/IEC15408. When realizing MMC110 and using it by a actual electronic payment service etc. by adding the function to perform security processing to MMC, MMC110 needs to receive the evaluation and authorization by evaluation and a certificate authority of ISO/IEC15408 similarly. In this invention, MMC110 builds in the attested IC card chip 150 by evaluation and a certificate authority, and obtains a security processing function by having the structure of performing security processing using the IC card chip 150. Therefore, MMC110 can satisfy the security valuation basis based on ISO/IEC15408 easily, and can shorten the development cycle for adding a security processing function to MMC.

[0026]As for MMC110, it is preferred to have an external interface based on MMC specification. MMC110 leads one kind of external interface -- a standard memory card command (command for accessing to the flash memory chip 130) -- in addition, it is necessary to receive the command which performs security processing The controller chip 120 chooses the chip which should be accessed by whether the command which MMC110 received is a standard memory card command, or it is a command which performs security processing, and has a function which distributes command processing. In this embodiment, if the controller chip 120 receives a standard memory card command, it chooses the flash memory chip 130, publishes a flash plate memory command to this, and can write host data. [reading and] If the command which performs security processing is received, the IC card chip 150 can be chosen, an IC card command can be published to this, and security processing can be performed.

[0027]As for the external terminal of the IC card chip 150, except for the ground terminal, the power supply terminal, the clock input terminal, the reset input terminal, and the I/O input/output terminal are connected with the controller chip 120.

[0028]The controller chip 120 lets a power supply terminal and a clock input terminal pass, and controls the current supply to the IC card chip 150, and clock supply. According to this embodiment, when security processing is not required from the host equipment 220, the controller chip 120 can suspend the current supply to the IC card chip 150, and clock supply, and the power consumption of MMC110 can be reduced.

[0029]In order to change into the state where an IC card command is receivable the IC card chip 150 to which the power supply is not supplied, it is necessary to start current supply to the IC card chip 150, and to perform reset processing first. The controller chip 120 has a function in which MMC110 starts the current supply to the IC card chip 150 through a power supply terminal ignited by having received the command which performs security processing from the host equipment 220. The controller chip 120 has a function in which MMC110 performs reset processing of the IC card chip 150 through a reset input terminal ignited by having received the command which performs security processing from the host equipment 220. According to this embodiment, the controller chip 120 can stop the current supply to the IC card chip 150 until it receives the command which performs security processing. Therefore, the power consumption of MMC110 is reducible.

[0030]The controller chip 120 generates the clock signal supplied to the IC card chip 150 through the clock input terminal of the IC card chip 150 in MMC110 inside, and has a function which controls the frequency, supply start timing, and supply interruption timing. According to this embodiment, since it can be made unrelated to the clock signal of the clock input terminal of the MMC external terminal

140, security improves to the attacking method called the timing analysis by the host equipment 220, power difference part analysis, and failure use analysis.
[0031]Drawing 21 is a figure showing the internal configuration of the flash memory chip 130. The flash memory chip 130 has the host data area 2115 and the management domain 2110. The host data area 2115 is a field where the logical address is mapped per sector, and the host equipment 220 is a field which specifies a logical address and can write data.
[0032]The host data area 2115 has the user file field 2130 and the security processing application area 2120. The user file field 2130 is a field where reading and a user can write file data freely. The security processing application area 2120, The host equipment 220 is a field which stores data required for security processing application, and user access restriction is logically applied by the security processing application of the host equipment 220 so that a user may not access unjustly. As data stored here, an application program of the host equipment 220, There are data only for the application, certificates (for example, an electronic banking application program, electronic banking log information, an electronic payment service certificate, etc.) used for security processing, etc. Since MMC110 stores the data used when the host equipment 220 performs security processing instead of the host equipment 220 according to this embodiment, convenience improves for the host equipment 220.
[0033]The management domain 2110 is a field which stores information for the controller chip 120 to manage the IC card chip 150. The management domain 2110 has the IC card control-parameter field 2111, the IC card configuration information area 2112, the CLK2 setup-information field 2113, the security processing buffer space 2114, and the security processing status areas 2116. The detailed directions of the field of 2111-2116 are mentioned later.
[0034]The controller chip 120 uses the security processing buffer space 2114 of the management domain 2110 of the flash memory chip 130 as the main memory or the buffer memory at the time of performing security processing by the IC card chip 150. When the host equipment 220 accesses MMC110 by the command which performs security processing, If the security associated data of the big size like [MMC110 cannot transmit to the IC card chip 150 at once from the host equipment 220] is received, The controller chip 120 stores temporarily in the security processing buffer space 2114 with sufficient capacity the data which chose access to the flash memory chip 130, and was received. Size to the extent that it cannot transmit to the IC card chip 150 at once is the size exceeding the allowable data size (for example, 255 bytes or 256 bytes) of an IC card command. And the controller chip 120 divides it into the data of size which can be transmitted to the IC card chip 150, reads divided data from the flash memory chip 130, and transmits to the IC card chip 150 gradually. That is, read-out of the divided data and writing are repeated. Since the security associated data of the big size for the host equipment 220 can be treated according to this embodiment, the convenience of security processing improves.
[0035]Host access restrictions are physically applied by the controller chip 120 so that the host equipment 220 may access unjustly the management domain 2110 including the security processing buffer space 2114 and security processing cannot be analyzed. That is, in the management domain 2110, reading and the host equipment 220 cannot write immediate data. According to this embodiment, since the host equipment 220 cannot read the contents of the security processing buffer space 2114 freely or it cannot alter, the reliability and the safety of security processing improve.
[0036]Drawing 23 is a figure showing the security processing of contents distribution as an example using MMC110 of security processing. The content provider 2310 is a contractor who sells the contents 2314 to the user who owns MMC110. The host equipment 220 is a terminal connectable via a network etc. with the content provider 2310 in this example. A user connects MMC110 to the host equipment 220, and purchases the contents 2314. Hereafter, the procedure is explained.
[0037]First, the host equipment 220 publishes the command which reads the user certificate 2321 stored in the flash memory chip 130 to MMC110. The controller chip 120 of MMC110 reads the user certificate 2321 stored in the security processing application area 2120 of the flash memory chip 130, and transmits it to the host equipment 220. The host equipment 220 which received the user certificate 2321 transmits it to the content provider 2310. The content provider 2310 verifies the digital signature attached to the user certificate 2321 (2311). If verification is successful, the content provider 2310 will generate a session key with a random number generator (2312), and it will encipher by the user public key which extracted it from the user certificate 2321 (2313). The content provider 2310 enciphers the contents 2314 with a session key (2315). The content provider 2310 transmits the result of Step 2313 to the host equipment 220.

[0038]The host equipment 220 publishes to MMC110 the command which requires the security processing which decodes the result of Step 2313 with the user secret key 2322. The controller chip 120 publishes the IC card command which decodes the result of Step 2313 with the user secret key 2322 to the IC card chip 150. With the user secret key 2322, the IC card chip 150 decodes the result of Step 2313, and acquires a session key (2323). The host equipment 220 publishes to MMC110 the command to which the information which shows whether this decoding processing was successful is made to output. The controller chip 120 builds the information which the host equipment 220 searches for based on the decoding result (IC card response which shows whether decoding processing was successful) which the IC card chip 150 outputs. And MMC110 transmits the information to the host equipment 220.
[0039]Next, the content provider 2310 transmits the result of Step 2315 to the host equipment 220. The host equipment 220 publishes to MMC110 the command which requires the security processing which decodes the result of Step 2313 with a session key (key acquired by Step 2323). The controller chip 120 publishes the IC card command which decodes the result of Step 2315 with a session key to the IC card chip 150. With a session key, the IC card chip 150 decodes the result of Step 2315, and restores the contents 2314 (2324). The controller chip 120 receives these contents 2314 from the IC card chip 150, and writes them in the flash memory chip 130. The host equipment 220 publishes to MMC110 the command to which the information which shows whether this decoding processing was successful is made to output. The controller chip 120 builds the information which the host equipment 220 searches for based on the decoding result (IC card response which shows whether decoding processing was successful) which the IC card chip 150 outputs. And MMC110 transmits the information to the host equipment 220. If the host equipment 220 tells the content provider 2310 having received contents safely, the content provider 2310 will charge a content rate at the user written in the user certificate. The user can read and use the contents 2314 stored in the flash memory chip 130 in MMC110 with the host equipment 220. Many contents can be purchased if a mass flash memory is used for the storage of the flash memory chip 130. According to this embodiment, both the security processing in contents distribution and contents storage are easily realizable by MMC110. Settlement of a content rate may be performed using the IC card chip 150.
[0040]Drawing 24 and drawing 25 are SD cards (24 millimeters in width, 32 millimeters in length, thickness 2.) about this invention, respectively. it is a sized memory card which had nine external terminals and carries a flash memory at 1 millimeter. and an internal configuration when it applies to a memory stick (a memory stick is a registered trademark of Sony Corp.) -- a table -- the bottom is a figure.
[0041]SD card 2410 which applied this invention has the SD card controller chip 2420, the flash memory chip 2430, the SD card external terminal 2440, and the IC card chip 150. The memory stick 2510 which applied this invention has the memory stick controller chip 2520, the flash memory chip 2530, the memory stick external terminal 2540, and the IC card chip 150.
[0042]The flash memory chips 2430 and 2530 are memory chips which use nonvolatile semiconductor memory as a storage, and can perform reading and writing of data with a flash plate memory command. The SD card controller chip 2420 and the memory stick controller chip 2520 are microcomputer chips which control other components in an SD card and a memory stick, respectively.

[0043]The SD card external terminal 2440, It has nine terminals located in a line from an end in order of the Data2 terminal 2441, the Data3 terminal 2442, the Com terminal 2443, the Vss terminal 2444, the Vdd terminal 2445, the Clock terminal 2446, the Vss terminal 2447, the Data0 terminal 2448, and the Data1 terminal 2449. The Vdd terminal 2445 a power supply terminal and the Vss terminals 2444 and 2447 A ground terminal, As for the Data0 terminal 2448, the Data1 terminal 2449, the Data2 terminal 2441, and the Data3 terminal 2442, a command input/output terminal and the Clock terminal 2446 of a data input/output terminal and the Com terminal 2443 are clock input terminals. Although SD card 2410 differs in interface specification with the SD card host equipment 2460 connected outside from MMC110, Since it has the MMC external terminal 140 and a dramatically similar external terminal and has the feature which operates by publishing a command from the exterior like MMC110, this invention is applicable.
[0044]On the other hand, the memory stick external terminal 2540, The Gnd terminal 2541, the BS terminal 2542, Vcc terminal 2543, and the one request-to-print-out-files terminal Rsv are flown from an end. It has ten terminals which fly the DIO terminal 2544, the INS terminal 2545, and the one request-to-print-out-files terminal Rsv, and are located in a line in order of the SCK terminal 2546, Vcc terminal 2547, and the Gnd terminal 2548. As for a power supply terminal and the Gnd terminals

2541 and 2548, a command and a data input/output terminal, and the SCK terminal 2546 of a ground terminal and the DIO terminal 2544 are [Vcc terminals 2543 and 2547] clock input terminals. Although the memory stick 2510 differs in interface specification with the memory stick host equipment 2560 connected outside from MMC110, since it has the feature which operates by publishing a command from the exterior like MMC110, it can apply this invention.

[0045]Drawing 1 is a figure showing the internal configuration of MMC110 which applied this invention. Drawing 2 is a figure showing the composition and the connected state of the host equipment 220 linked to MMC110 of drawing 1. The host equipment 220 has the VCC1 power supply 221, CLK 1-phase oscillator 222, and the host interface 223.

[0046]MMC110 has the MMC external terminal 140 for exchanging information with the external host equipment 220. The MMC external terminal 140 has seven terminals of the CS terminal 141, the CMD terminal 142, the GND1 terminals 143 and 146, the VCC1 terminal 144, the CLK1 terminal 145, and the DAT terminal 147. MMC specification has specified two kinds of an MMC mode and SPI mode as operational mode of MMC110, and the directions of the MMC external terminal 140 change with operational modes. This example explains the case of operation by an MMC mode in detail.

[0047]It is connected with the VCC1 power supply 221, and the VCC1 terminal 144 is a power supply terminal for the host equipment 220 to supply electric power to MMC110. It is connected with the VCC1 power supply 221, and the GND1 terminals 143 and 146 are electric ground terminals of MMC110. The GND1 terminal 143 and the GND1 terminal 146 are electrically short-circuited by MMC110 inside.

[0048]It is connected to the host interface 223 and the CS terminal 141 is an input terminal used in operation in SPI mode. L level is inputted into the CS terminal 141 when the host equipment 220 accesses MMC110 in SPI mode. It is not necessary to use the CS terminal 141 in operation of an MMC mode. The CMD terminal 142 is connected to the host interface 223, The host equipment 220 is an input/output terminal used in order to transmit the memory card command based on memory card interface specification to MMC110 or to receive the memory card response based on the specification from MMC110. The DAT terminal 147 is connected to the host interface 223, The host equipment 220 is an input/output terminal used in order to transmit the input data of the form based on memory card interface specification to MMC110 or to receive the output data of the form based on the specification from MMC110.

[0049]It is connected to CLK 1-phase oscillator 222, and the CLK1 terminal 145 is a terminal into which the clock signal which CLK 1-phase oscillator 222 generates is inputted. A clock signal is inputted into the CLK1 terminal 145, when the host equipment 220 transmits and receives a memory card command and a memory card response through the CMD terminal 142 or transmits and receives host data through the DAT terminal 147. The clock signal is supplied to the host interface 223 from CLK 1-phase oscillator 222, and a memory card command, a memory card response, and host data, Synchronizing with the clock signal which CLK 1-phase oscillator 222 generates, between the host equipment 220 and MMC110 is transmitted by bitwise.

[0050]MMC110 has the controller chip 120. The controller chip 120 has CPU121, the flash memory I/F control circuit 122, the MMCI/F control circuit 123, CLK 0-phase oscillator 124, the VCC2 generation machine 125, the VCC2 control circuit 126, the CLK2 control circuit 127, and the IC card I/F control circuit 128. These components 121-128 operate with the electric power supplied through the VCC1 terminal 144 and the GND1 terminals 143 and 146 from the host equipment 220. It is connected with the CS terminal 141, the CMD terminal 142, the CLK1 terminal 145, and the DAT terminal 147, and the MMCI/F control circuit 123 is a logic circuit which controls an interface for MMC110 to exchange information with the host equipment 220 through those terminals.

[0051]It is connected with the MMCI/F control circuit 123, and CPU121 controls the MMCI/F control circuit 123. When the MMCI/F control circuit 123 receives a memory card command from the host equipment 220 through the CMD terminal 142, the MMCI/F control circuit 123, In order to tell the result of whether reception of the command was successful to the host equipment 220, a response is transmitted to the host equipment 220 through the CMD terminal 142. CPU121 interprets the received memory card command and performs processing according to a command content. When data needs to be transmitted and received through the host equipment 220 and the DAT terminal 147 according to the command content, CPU121 acquires the data from sending out of the data to the MMCI/F control circuit 123, and the MMCI/F control circuit 123. CPU121 also controls the data transfer procedure between the MMCI/F control circuit 123 and the host equipment 220. For example, CPU121 makes L level output to the DAT terminal 147, and it tells that MMC110 is a busy state to the host equipment 220 so that the host equipment 220 may not suspend the current supply

of MMC110 during processing of the data received from the host equipment 220. It is connected with CPU121 and CLK 0-phase oscillator 124 supplies the driving clock which operates CPU121.
[0052]MMC110 has the flash memory chip 130. The flash memory chip 130 is a memory chip which uses nonvolatile semiconductor memory as a storage. The flash memory chip 130 operates with the electric power supplied through the VCC1 terminal 144 and the GND1 terminals 143 and 146 from the host equipment 220. The flash memory chip 130 has a write function which stores the inputted data in nonvolatile semiconductor memory, and a lead function which outputs outside the data stored in the memory according to the flash plate memory command from the outside. The flash memory I/F control circuit 122 is a logic circuit for publishing a flash plate memory command to the flash memory chip 130, or transmitting the data outputted and inputted by the command to it. CPU121 controls the flash memory I/F control circuit 122, and makes the flash memory chip 130 perform the write function and lead function of data. When it is necessary to carry out the light of the data received from the host equipment 220 to the flash memory chip 130, or to transmit the data stored in the flash memory chip 130 to the host equipment 220, CPU121 controls the data transfer between the flash memory I/F control circuit 122 and the MMCI/F control circuit 123.
[0053]MMC110 has the IC card chip 150. The IC card chip 150 is an IC chip designed for the purpose of embedding into the substrate of an IC card, and has eight external terminals based on the external terminal standard of the IC card. Among these, directions are assigned by the external terminal standard of the IC card, and six terminals are reserve terminals for the remaining future [two]. The six terminals are the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, the GND2 terminal 155, the VPP terminal 156, and the I/O terminal 157.
[0054]The ground terminal of the IC card chip 150 is connected to GND1 (ground terminal) 146 of the MMC external terminal 140. The VCC2 terminal (power input terminal) 151 of the IC card chip 150 is connected to the VCC2 control circuit 126 of the controller chip 120. The RST terminal (reset input terminal) 152 and the I/O terminal (data input/output terminal) 157 of the IC card chip 150 are connected to the IC card I/F control circuit 128 of the controller chip 120. The CLK2 terminal (clock input terminal) 153 of the IC card chip 150 is connected to the CLK2 control circuit 127 of the controller chip 120.
[0055]The VCC terminal (power input terminal) of the flash memory chip 130 is connected to VCC1144 of the MMC external terminal 140. The VSS terminal (ground terminal) of the flash memory chip 130 is connected to GND1146 of the MMC external terminal 140. The I/O terminal (data input/output terminal), a lady/busy terminal, the chip enable terminal, the output enable terminal, the write enable terminal, clock terminal, and reset terminal of the flash memory chip 130, It is connected to the flash memory IF control circuit 122 of the controller chip 120.
[0056]The VCC2 terminal 151 is a power supply terminal for supplying electric power to the IC card chip 150. The VCC2 control circuit 126 is a circuit which controls a supply start and supply interruption of the electric power to the VCC2 terminal 151 by the switching circuit which used the MOS-FET element. The VCC2 generation machine 125 generates the voltage supplied to the VCC2 terminal 151, and supplies it to the VCC2 control circuit 126. The electrical signal standard of an IC card has specified the class A and the class B as a class of an IC card of operation. The standard voltage supplied to the VCC2 terminal 151 is 3V in 5V and the class B in the class A. Although cannot depend this invention and it can be applied to the class of the IC card chip 150 of operation, this example explains in detail the case where the IC card chip 150 operates in the class B.
[0057]The VPP terminal 156 is a terminal which supplies the variable voltage used in order to write data in internal nonvolatile memory or to eliminate when the IC card chip 150 operates in the class A, and when operating in the class B, it is not used. The GND2 terminal 155 is an electric ground terminal of the IC card chip 150, and is connected with the GND1 terminals 143 and 146 too hastily. The VCC2 control circuit 126 is connected with CPU121, and CPU121 can control a start and stop of the electric power supply to the VCC2 terminal 151. When not using the IC card chip 150, CPU121 can stop the electric power supply to the VCC2 terminal 151. MMC110 can save the electric power which it consumes by stopping the electric power supply to the IC card chip 150. However, a stop of an electric power supply will not maintain the internal state of the IC card chip 150 except for the data memorized by the nonvolatile memory of IC card chip 150 inside.
[0058]The CLK2 terminal 153 is a terminal which inputs a clock signal into the IC card chip 150. The CLK2 control circuit 127 is a circuit which supplies a clock to the CLK2 terminal 153. The CLK2 control circuit 127 generates the clock signal supplied to the CLK2 terminal 153 based on the clock signal supplied from CLK 0-phase oscillator 124. It is connected with CPU121 and the CLK2 control circuit 127 can control a supply start and supply interruption of the clock to the CLK2 terminal 153

from CPU121. The IC card chip 150 does not have a driving clock oscillator in the inside of self. Therefore, it operates by supplying a driving clock from the CLK2 terminal 153. Since the CLK2 control circuit 127 will suspend operation of the IC card chip 150 if it suspends clock supply for the CLK2 terminal 153, the power consumption of the IC card chip 150 can be reduced. If the electric power supply to the VCC2 terminal 151 is maintained at this time, the internal state of the IC card chip 150 will be maintained.

[0059]If F0, P, and Q are made into a positive integer, the frequency of the clock signal to which the frequency of the clock signal supplied to the CLK2 terminal 153 was supplied from F2 and CLK 0-phase oscillator 124 here, The CLK2 control circuit 127 creates a clock signal which becomes a relation of F2=(P/Q) *F0, and supplies this to the CLK2 terminal 153. The value of P and Q can be set up now by CPU121. If P is set up greatly and F2 is enlarged, the internal processing of the IC card chip 150 can be driven more at a high speed. If Q is set up greatly and F2 is made small, the internal processing of the IC card chip 150 can be driven more at a low speed, and can reduce the power consumption of the IC card chip 150. The driving clock frequency of the IC card chip 150 needs to be set up in the permission frequency range where the IC card chip 150 can operate correctly. Therefore, the CLK2 control circuit 127 has the feature to which a value of P and Q in which the value of F2 separates from the permission frequency range is not made to set.

[0060]The I/O terminal 157 is an input/output terminal used when an IC card command is inputted into the IC card chip 150 or the IC card chip 150 outputs an IC card response. It is connected with the I/O terminal 157 and the IC card I/F control circuit 128 is a circuit which performs signal transmission of an IC card command, and signal reception of an IC card response through the I/O terminal 157. The IC card I/F control circuit 128 is connected to CPU121, and CPU121, Control the procedure of transmission and reception of the IC card command by the IC card I/F control circuit 128, or an IC card response, or, The IC card command data which should transmit are set as the IC card I/F control circuit 128, or the received IC card response is acquired from the IC card I/F control circuit 128. The clock is supplied to the IC card I/F control circuit 128 from the CLK2 control circuit 127, and it is transmitted [an IC card command or an IC card response] and received through the I/O terminal 157 synchronizing with the clock signal supplied to the CLK2 terminal 153 by bitwise. The RST terminal 152 is a terminal which inputs a reset signal, when resetting the IC card chip 150. It is connected with the RST terminal 152 and the IC card I/F control circuit 128 can send a reset signal to the IC card chip 150 with directions of CPU121.

[0061]The IC card chip 150 exchanges information based on the electrical signal standard and command standard of an IC card. The number of the access patterns to the IC card chip 150 is four, and they explain each pattern using drawing 3 - drawing 6. In the process (it is hereafter called cold reset) of the IC card chip 150 starting from a non-active state (state where the power supply is intercepted), with directions of CPU121, and initializing an internal state, drawing 3 is the figure which expressed simply the signal wave form of the external terminal of the IC card chip 150. In the process (it is hereafter called warm reset) in which the IC card chip 150 initializes an internal state by an active state (state where the power supply is supplied), with directions of CPU121, drawing 4 is the figure which expressed simply the signal wave form of the external terminal of the IC card chip 150. In the process of transmitting an IC card command to the IC card chip 150 with directions of CPU121, and receiving an IC card response from the IC card chip 150, drawing 5 is the figure which expressed simply the signal wave form of the external terminal of the IC card chip 150. In the process of making the IC card chip 150 into a non-active state with directions of CPU121, drawing 6 is the figure which expressed simply the signal wave form of the external terminal of the IC card chip 150. In drawing 3 - drawing 6, the direction of time is taken on the right from the left, and the signal observed toward a lower line with the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the upper line is expressed. A dashed line expresses the standard (L level) of each signal.

[0062]With reference to drawing 3, cold reset operation of the IC card chip 150 is explained. First, the IC card I/F control circuit 128 uses the RST terminal 152 as L level (301). Next, the VCC2 control circuit 126 starts the current supply to VCC2 terminal (302). Next, the CLK2 control circuit 127 starts supply of the clock signal to the CLK2 terminal 153 (303). Next, the IC card I/F control circuit 128 changes the I/O terminal 157 into the state Z (state by which pull-up was carried out) (304). Next, the IC card I/F control circuit 128 uses the RST terminal 152 as H level (305). Next, the IC card I/F control circuit 128 starts reception of the reset response outputted from the I/O terminal 157 (306). If reception of a reset response is completed, the CLK2 control circuit 127 will suspend supply of the clock signal to the CLK2 terminal 153 (307). Now, operation of cold reset is completed. Step

307 is a device for reducing power consumption, and may be skipped.
[0063]With reference to drawing 4, the warm reset action of the IC card chip 150 is explained. First, the CLK2 control circuit 127 starts supply of the clock signal to the CLK2 terminal 153 (401). Next, the IC card I/F control circuit 128 uses the RST terminal 152 as L level (402). Next, the IC card I/F control circuit 128 changes the I/O terminal 157 into the state Z (403). Next, the IC card I/F control circuit 128 uses the RST terminal 152 as H level (404). Next, the IC card I/F control circuit 128 starts reception of the reset response outputted from the I/O terminal 157 (405). If reception of a reset response is completed, the CLK2 control circuit 127 will suspend supply of the clock signal to the CLK2 terminal 153 (406). Now, operation of warm reset is completed. Step 406 is a device for reducing power consumption, and may be skipped.
[0064]With reference to drawing 5, operation of transmitting an IC card command to the IC card chip 150, and receiving an IC card response from the IC card chip 150 is explained. First, the CLK2 control circuit 127 starts supply of the clock signal to the CLK2 terminal 153 (501). Step 501 is unnecessary when the clock is already supplied. Next, the IC card I/F control circuit 128 starts transmission of command data for the I/O terminal 157 (502). If transmission of command data is completed, the IC card I/F control circuit 128 will change the I/O terminal 157 into the state Z (503). Next, the IC card I/F control circuit 128 starts reception of the response data outputted from the I/O terminal 157 (504). If reception of response data is completed, the CLK2 control circuit 127 will suspend supply of the clock signal to the CLK2 terminal 153 (505). Now, operation of IC card command transmission and IC card response reception is completed. Step 505 is a device for reducing power consumption, and may be skipped.
[0065]With reference to drawing 6, the operation which deactivates the IC card chip 150 is explained. First, the CLK2 control circuit 127 uses the CLK2 terminal 153 as L level (601). Next, the IC card I/F control circuit 128 uses the RST terminal 152 as L level (602). Next, the IC card I/F control circuit 128 uses the I/O terminal 157 as L level (603). Finally, the VCC2 control circuit 126 suspends the current supply to VCC2 terminal (604). Now, operation of deactivation is completed.
[0066]The IC card chip 150 has the security processing function to perform a code operation required for security data protection, personal authentication, etc. The IC card chip 150 exchanges information, when an IC card command and an IC card response transmit and receive between CPU121, and it performs the result of calculation, sending out of the information memorized, change of the information memorized, etc. as the result. CPU121 can perform security processing using the IC card chip 150. If MMC110 receives a specific memory card command from the host equipment 220, CPU121 ignited by it control the current supply to the IC card chip 150 through the VCC2 control circuit 126, or, Or the clock supply to the IC card chip 150 is controlled through the CLK2 control circuit 127, or an IC card command is transmitted to the IC card chip 150 through the IC card I/F control circuit 128. Thereby, CPU121 performs security processing which the host equipment 220 requires using the IC card chip 150. CPU121 may perform security processing ignited by reception of a specific memory card command by operating it, combining the power supply control, the clock supply control, IC card command transmission, and IC card response reception to the IC card chip 150 two or more. CPU121 may perform security processing ignited by the host equipment 220 having started current supply to MMC110. The result of security processing uses as a base the IC card response which the IC card chip 150 outputs, is constituted, and is held in MMC110. If MMC110 receives a specific memory card command from the host equipment 220, CPU121 will transmit the result of security processing to the host equipment 220 ignited by it.
[0067]Drawing 7 expresses a flow chart in case the host equipment 220 accesses MMC110. First, the host equipment 220 starts current supply for the VCC1 terminal 144, in order to activate MMC110 (701). MMC110 performs the first IC card initialization processing ignited by this (702). The details of the first IC card initialization processing are mentioned later. Next, since MMC110 is initialized, the host equipment 220 transmits the initialization commands of MMC110 through the CMD terminal 142 (703). Two or more kinds of these initialization commands exist based on MMC specification. Since MMC110 is initialized, the host equipment 220 may transmit two or more initialization commands. If MMC110 receives initialization commands, MMC110 will process it (704). MMC110 performs the second IC card initialization processing ignited by this (705). The details of the second IC card initialization processing are mentioned later.
[0068]The host equipment 220 receives the memory card response to the initialization commands of MMC110 through the CMD terminal 142, and judges whether initialization of MMC110 was completed from the contents of the memory card response. If it has not completed, initialization commands will be transmitted again (703). If initialization of MMC110 is completed, the host equipment 220, The

standard memory card command (command for accessing to the flash memory chip 130) based on MMC specification, It moves from transmission of the specific memory card command (command for accessing to the IC card chip 150) relevant to the security processing described above to the state of standing by (707). In this waiting state, the host equipment 220 can transmit a standard memory card command (708). If MMC110 receives a standard memory card command, MMC110 will process it (709). If processing is completed, the host equipment 220 will return to a waiting state again (707). In this waiting state, the host equipment 220 can also transmit a security processing demand write command (710). A security processing demand write command is one sort of the specific memory card command relevant to the security processing described above, and in order that it may make MMC110 perform security processing, it is a memory card command which transmits a processing demand.

[0069]If MMC110 receives a security processing demand write command, CPU121 will interpret the demanded contents of security processing and will describe security processing in the form of an IC card command (711). That is, CPU121 changes the standard memory card command from the host equipment 230 into the specific memory card command which the IC card chip 150 can interpret according to the rule defined beforehand. And the IC card command acquired as the result is published to the IC card chip 150, and demanded security processing is performed (712). If processing is completed, the host equipment 220 will return to a waiting state again (707). In this waiting state, the host equipment 220 can also transmit a security processing result read command (713). A security processing result read command is one sort of the specific memory card command relevant to the security processing described above, and in order to know the executed result of the security processing by MMC110, it is a memory card command which receives a processing result.

[0070]If MMC110 receives a security processing result read command, CPU121 will build the security processing result which should transmit to the host equipment 220 based on the IC card response received from the IC card chip 150 (714). And the host equipment 220 receives a security processing result from MMC110. If reception is completed, the host equipment 220 will return to a waiting state again (707). Step 714 may be performed in Step 712.

[0071]In drawing 7, the first IC card initialization processing and the second IC card initialization processing which are performed at Step 702 and Step 705 are processing which it prepares for performing security processing within MMC110, and CPU121 accesses to the IC card chip 150. Specifically, activation of the IC card chip 150, deactivation, reset of the IC card chip 150, and configuration of the IC card chip 150 are performed. The information which needs configuration in order to perform security processing. It means reading (for example, the information on an usable cryptographic algorithm, the information about the secret key and public key which are used for code calculation, the information about the authentication data used for personal authentication, etc.) from the IC card chip 150, or writing them in the IC card chip 150.

[0072]Configuration of the IC card chip 150 is performed to the IC card chip 150 by carrying out N piece (N is positive integer) issue of the IC card command. For example, if three session keys are necessary, an IC card command will be published 3 times, and if two session keys are necessary, an IC card command will be published twice. N IC card commands may be mutually different, and may be the same. It was not fixed and the value of N turns into various values by a situation. Hereafter, the IC card command published by configuration is called a setting command. The IC card command which performs security processing based on this configuration is hereafter called a security command. There is a command which performs calculation of a digital signature, verification of a digital signature, encryption of a message, decoding of an encryption message, attestation with a password, etc. as an example of a security command.

[0073]CPU121 can change the contents of the configuration of the IC card chip 150 freely. CPU121 may change this according to the contents of security processing, or a result, and may change this ignited by reception of the memory card command from host equipment. CPU121 carries out the light of the information which showed the contents of configuration to the flash memory chip 130, and when required, it can also lead and use the information from the flash memory chip 130. This information is shown as the IC card configuration information 2112 in drawing 21. The time and effort anew set up whenever it can hold the information and MMC110 is activated, even if MMC110 is deactivated by this can be saved.

[0074]The first IC card initialization processing and the second IC card initialization processing are performed based on the value set as IC card control-parameter A, B, and C. In the security processing performed at Step 712, CPU121 controls activation and deactivation of the IC card chip 150 based on the value set as IC card control-parameter D.

[0075]Drawing 8 expresses the kind of IC card control parameter, and the contents of the processing corresponding to a preset value and it. First, the parameter A is a parameter about the first IC card initialization processing performed when a power supply is supplied to MMC110. At the time of A= 0, CPU121 is not accessed at the IC card chip 150. At the time of A= 1, CPU121 carries out cold reset of the IC card chip 150. At the time of A= 2, CPU121 performs configuration of the IC card chip 150, after carrying out cold reset of the IC card chip 150. At the time of A= 3, CPU121 performs configuration of the IC card chip 150, after carrying out cold reset of the IC card chip 150, and finally it deactivates the IC card chip 150. At the time of A= 0 or A= 3, the IC card chip 150 will be in a non-active state after the first IC card initialization processing. At the time of A= 1 or A= 2, the IC card chip 150 will be in an active state after the first IC card initialization processing.
[0076]Next, the parameters B and C are parameters about the second IC card initialization processing performed when MMC110 processes MMC initialization commands. At the time of B= 0, CPU121 is not accessed at the IC card chip 150. At the time of B= 1 and C= 1, CPU121 resets the IC card chip 150 (cold reset or warm reset). At the time of B= 1 and C= 2, CPU121 performs configuration of the IC card chip 150, after resetting the IC card chip 150. At the time of B= 1 and C= 3, CPU121 performs configuration of the IC card chip 150, after resetting the IC card chip 150, and finally it deactivates the IC card chip 150. At the time of B= 2 and C= 2, CPU121 performs configuration of the IC card chip 150. At the time of B= 2 and C= 3, CPU121 deactivates the IC card chip 150, after performing configuration of the IC card chip 150. If the IC card chip 150 is an active state at the time of B= 3, CPU121 will deactivate the IC card chip 150.
[0077]Finally, the parameter D is a parameter which shows whether the IC card chip 150 is deactivated, after performing security processing demanded from the host equipment 220. After execution of security processing, the IC card chip 150 is not deactivated at the time of D= 0, but it maintains CPU121 at an active state. At the time of D= 1, CPU121 deactivates the IC card chip 150 after execution of security processing.
[0078]CPU121 can change the preset value of IC card control-parameter A, B, C, and D. CPU121 may change these preset values according to the contents of security processing, or a result, and may change these preset values ignited by reception of the memory card command from host equipment. CPU121 carries out the light of these preset values to the flash memory chip 130, and when required, it can also lead and use these preset values from the flash memory chip 130. These preset values are shown as the IC card control parameter 2111 in drawing 21. The time and effort anew set up whenever it can hold these preset values and MMC110 is activated, even if MMC110 is deactivated by this can be saved.
[0079]Drawing 9 is a flow chart which shows the procedure of the first IC card initialization processing. initialization processing -- starting (901) -- IC card control-parameter A checks in 0 first (902). If it becomes A=0, initialization processing will be ended as it is (908). If it is not A= 0, cold reset of the IC card chip 150 will be carried out (903). Next, IC card control-parameter A checks in 1 (904). Initialization processing will be ended if it becomes A=1 (908). If it is not A= 1, configuration of the IC card chip 150 will be performed (905). Next, IC card control-parameter A checks in 2 (906). Initialization processing will be ended if it becomes A=2 (908). If it is not A= 2, the IC card chip 150 will be deactivated (907). And initialization processing is ended (908).
[0080]Drawing 10 is a flow chart which shows the procedure of the second IC card initialization processing. initialization processing -- starting (1001) -- IC card control-parameter B checks in 0 first (1002). If it becomes B=0, initialization processing will be ended as it is (1013). If it is not B= 0, it will check in B= 1 (1003). If it becomes B=1, IC card control-parameter A will check in 0 or 3 (1004). A -- 0 -- or if it becomes three, cold reset of the IC card chip 150 will be carried out (1005), and it will move to Step 1007. A -- 1 -- or if it becomes two, the IC card chip 150 will be warm reset (1006), and it will move to Step 1007. In Step 1007, IC card control-parameter C checks in 1. Initialization processing will be ended if it becomes C=1 (1013). If it is not C= 1, it will move to Step 1009. If it is not B= 1 in Step 1003, B will check in 2 (1008). If it becomes B=2, it will move to Step 1009. If it is not B= 2, IC card control-parameter A will check in 0 or 3 (1011). A -- 0 -- or initialization processing will be ended if it becomes three (1013). A -- 1 -- or if it becomes two, it will move to Step 1012. Configuration of the IC card chip 150 is performed at Step 1009. And IC card control-parameter C checks in 2 (1010). Initialization processing will be ended if it becomes C=2 (1013). If it is not C= 2, it will move to Step 1012. The IC card chip 150 is deactivated at Step 1012. And initialization processing is ended (1013).
[0081]Drawing 11 is the figure which expressed briefly the signal wave form of the external terminal of the IC card chip 150, when the IC card chip 150 is a non-active state and the first IC card

initialization processing or the second IC card initialization processing is performed. Drawing 12 is the figure which expressed briefly the signal wave form of the external terminal of the IC card chip 150, when the IC card chip 150 is an active state and the second IC card initialization processing is performed. In drawing 11 and drawing 12, the direction of time is taken on the right from the left, and the signal observed toward a lower line with the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the upper line is expressed. A lateral dashed line expresses the standard (L level) of each signal.

[0082]In drawing 11, 1102 expresses the signal wave form of the cold reset shown in drawing 3. In drawing 12, 1202 expresses the signal wave form of the warm reset shown in drawing 4. In drawing 11 and drawing 12, the 1st setting command processings 1104a and 1204a, the 2nd setting command processings 1104b and 1204b, and the Nth setting command processings 1104c and 1204c express the signal wave form of the IC card command processing shown in drawing 5, respectively. The signal wave form of N setting command processings stands in a row, and the signal wave forms 1104 and 1204 of the configuration of the IC card chip 150 are constituted.

[0083]In drawing 11 and drawing 12, 1106 and 1206 express the signal wave form of the deactivation shown in drawing 6, respectively. In drawing 11 and drawing 12, the dashed lines 1101, 1103, 1105, 1107, 1201, 1203, 1205, and 1207 of a lengthwise direction express respectively specific time. The time in front of cold reset and 1201 1101 The time before warm reset, The time which has 1103 between in front of configuration after cold reset, the time which has 1203 between in front of configuration after warm reset, the time which has 1105 and 1205 in between before deactivation after configuration, and 1107 and 1207 are the time after deactivation.

[0084]With reference to drawing 11, the signal wave form at the time of the first IC card initialization processing execution is shown. When IC card control-parameter A is 0, it is changeless to a signal wave form. At the time of A= 1, it becomes a signal wave form of the range from the time 1101 to the time 1103. At the time of A= 2, it becomes a signal wave form of the range from the time 1101 to the time 1105. At the time of A= 3, it becomes a signal wave form of the range from the time 1101 to the time 1107.

[0085]With reference to drawing 11, the signal wave form at the time of the second IC card initialization processing execution in case IC card control-parameter A is 0 or 3 is shown. When IC card control-parameter B is 0, it is changeless to a signal wave form. At the time of B= 1 and the IC card control parameter C= 1, it becomes a signal wave form of the range from the time 1101 to the time 1103. At the time of B= 1 and C= 2, it becomes a signal wave form of the range from the time 1101 to the time 1105. At the time of B= 1 and C= 3, it becomes a signal wave form of the range from the time 1101 to the time 1107.

[0086]With reference to drawing 12, the signal wave form at the time of the second IC card initialization processing execution in case IC card control-parameter A is 1 or 2 is shown. When IC card control-parameter B is 0, it is changeless to a signal wave form. At the time of B= 1 and the IC card control parameter C= 1, it becomes a signal wave form of the range from the time 1201 to the time 1203. At the time of B= 1 and C= 2, it becomes a signal wave form of the range from the time 1201 to the time 1205. At the time of B= 1 and C= 3, it becomes a signal wave form of the range from the time 1201 to the time 1207. At the time of B= 2 and C= 2, it becomes a signal wave form of the range from the time 1203 to the time 1205. At the time of B= 2 and C= 3, it becomes a signal wave form of the range from the time 1203 to the time 1207. At the time of B= 3, it becomes a signal wave form of the range from the time 1205 to the time 1207.

[0087]Drawing 13 is a flow chart which shows a procedure in case CPU121 performs security processing which the host equipment 220 required by the IC card chip 150 in Step 712 of drawing 7. security processing -- starting (1301) -- the IC card chip 150 confirms first whether to be a non-active state (1302). If it is a non-active state, cold reset of the IC card chip 150 will be carried out (1303), and it will move to Step 1306. If it is an active state, it will move to Step 1304. In Step 1304, before publishing an IC card command to the IC card chip 150, it is confirmed whether it is necessary to re-reset the IC card chip 150. If there is necessity, the IC card chip 150 will be warm reset (1305), and it will move to Step 1306. If there is no necessity, it will move to Step 1306. In Step 1306, it is confirmed whether it is necessary to perform configuration of the IC card chip 150. If there is necessity, configuration of the IC card chip 150 will be performed (1307), and it will move to Step 1308. If there is no necessity, it will move to Step 1308. In Step 1308, the frequency F2 of the clock signal supplied to CLK2 terminal of the IC card chip 150 is set up. And CPU121 publishes a security command to the IC card chip 150, and the IC card chip 150 processes it (1309). It depends for the processing time of a security command on the clock frequency F2.

[0088]Next, it is judged whether the processing was successful by the IC card response which the IC card chip 150 outputs (1310). If it is a success, it will move to Step 1311. If it is failure, it will move to Step 1312. In Step 1311, it is confirmed whether all the security commands that should be published to the IC card chip 150 were completed. If there is still a security command which should be published, it will move to Step 1304. If all the security commands that should be published are completed, it will move to Step 1314. In Step 1312, it is judged whether it is possible to retry the security command which went wrong. If it can retry, retry setting out will be performed (1313) and it will move to Step 1304. Retry setting out is that CPU121 prepares again the security command which should be retried, and its associated data. If it cannot retry, it will move to Step 1314. This means what the security processing which the host equipment 220 required went wrong. IC card control-parameter D is checked in Step 1314. If it becomes D=1, the IC card chip 150 will be deactivated (1315) and security processing will be ended (1316). If it is not D= 1, security processing will be ended, maintaining the IC card chip 150 at an active state (1316).
[0089]In the flow chart of drawing 13, Step 1308 was located just before Step 1309 so that the clock frequency F2 could be changed according to the kind of security command published at Step 1309, but Step 1308 may be in the other position.
[0090]As one of the factors which validate the method of attacking the conventional IC card, it is raised that direct supply of the driving clock of an IC card is carried out from an external contact. Since a driving clock is under control of a contact, in a timing analysis or power difference part analysis, acquisition of the timing of IC card internal processing becomes easy in measurement of an electrical signal. On the other hand, in failure use analysis, generating of the arithmetic error by supply of an unusual driving clock becomes easy. On the other hand, according to this invention, when performing security processing by the IC card chip 150 by MMC110 inside, the host equipment 220 cannot carry out direct supply of the driving clock of the IC card chip 150. CPU121 can set up freely the frequency F2 of the clock supplied to the IC card chip 150. The security processing which corresponded to the processing performance which the host equipment 220 requires flexibly by this is realizable. What is necessary is to set up the frequency F2 highly, if security processing with the high-speed host equipment 220 is required, to set up the frequency F2 low, if low power consumption is required, or just to stop a clock moderately.
[0091]CPU121 can set up freely the supply start timing of not only the frequency F2 but a clock, and supply interruption timing. By changing these at random, the attacking method called the timing analysis, power difference part analysis, and failure use analysis to the IC card chip 150 can be made difficult. Since the timing analysis assumes that an aggressor can measure the processing time of one cipher processing correctly, as the measure, it is effective to prevent an aggressor from performing processing time Measurement Division correctly. The Reason a timing analysis becomes difficult by this invention is because the host equipment 220 cannot measure correctly the length of the time when the IC card chip 150 is processing the IC card command. It is effective to make the information about the execution timing and an order of processing undetectable from the exterior as a measure against power difference part analysis. Why power difference part analysis becomes difficult by this invention, It is because detection of the contents of the time when the IC card command was published, and the published IC card command, and an order (when performing security processing, combining an IC card command two or more) of the published IC card command becomes difficult for the host equipment 220. If operating environment detecting circuits, such as a clock, voltage, and temperature, are carried in an IC card and abnormalities are detected as a measure against failure use analysis, the method of making processing into a stop or use impossible is effective. The Reason failure use analysis becomes difficult by this invention is that that the CLK2 control circuit 127 does not supply an unusual driving clock to the IC card chip 150 prevents that the host equipment 220 makes the IC card chip 150 generate an arithmetic error.
[0092]CPU121 may change the preset value of the frequency F2 of the clock supplied to the IC card chip 150, supply start timing, and supply interruption timing according to the contents of security processing, or a result, and may change reception of the memory card command from host equipment as an opportunity. CPU121 carries out the light of these preset values to the flash memory chip 130, and when required, it can also lead and use these preset values from the flash memory chip 130. These preset values are shown as the CLK2 setup information 2113 in drawing 21. The time and effort anew set up whenever it can hold these preset values and MMC110 is activated, even if MMC110 is deactivated by this can be saved.
[0093]In a process (Steps 710-712 of drawing 7) after, as for drawing 14, the host equipment 220 publishes a security processing demand write command to MMC110 until security processing is

performed by the IC card chip 150, They are a signal wave form of the external terminal of MMC110 and the IC card chip 150, and the figure which expressed briefly access to the flash memory chip 130 by CPU121. In drawing 14, the direction of time is taken on the right from the left. The top lines are the contents of access to the flash memory chip 130. The signal observed toward a lower line with the VCC1 terminal 144, the CMD terminal 142, the CLK1 terminal 145, the DAT terminal 147, the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the line of the second line is expressed from a top. A lateral dashed line expresses the standard (L level) of each signal.

[0094]A process after the host equipment 220 publishes a security processing demand write command to MMC110 with reference to drawing 14 until security processing is performed by the IC card chip 150 is explained. First, the host equipment 220 transmits a security processing demand write command to the CMD terminal 142 (1401). Next, the host equipment 220 receives the response of a security processing demand write command from the CMD terminal 142 (1402). This response tells that MMC110 received the command to the host equipment 220, and is not an executed result of security processing. Next, the host equipment 220 transmits a security processing demand to the DAT terminal 147 (1403). A security processing demand is host data containing the contents and the data which should be processed of security processing. Next, MMC110 sets the DAT terminal 147 to L level (1404). It is shown in the host equipment 220 that MMC110 is a busy state by this. Next, CPU121 publishes the command which carries out the light of the security processing demand which received from the host equipment 220 to the flash memory chip 130 (1405). By carrying out the light of the security processing demand to the flash memory chip 130, CPU121 can save the amount of consumption of the work memory of CPU121 inside in the processing (Step 711 of drawing 7) which describes a security processing demand according to IC card command format. This is effective when the data size of a security processing demand is large.

[0095]The security processing demand by which the light was carried out to the flash memory chip 130 is stored in the security processing buffer space 2114 in drawing 21. The write command issue 1405 is not indispensable operation. The light processing term 1406 expresses the period when the flash memory chip 130 is performing light processing of a security processing demand. The security processing 1407 expresses the signal wave form of the security processing by the IC card chip 150. It depends for this signal wave form on the transition process of the flow chart of drawing 13. The security processing 1407 can be made to overlap the light processing term 1406. Generally, since the light processing term 1406 of the flash memory chip 130 is an order of a ms, it is effective for shortening of the overall processing time of security processing to make the security processing 1407 overlap. During execution of the security processing 1407, the read/write 1408 leads a security processing demand from the flash memory chip 130, or shows access which carries out the light of the calculation result which the IC card chip 150 outputted to the flash memory chip 130. This access can save the amount of consumption of the work memory of CPU121 inside. This is effective when the data size of a security processing demand or a security processing result is large. The read/write 1408 is not indispensable. If the security processing 1407 is completed, MMC110 will set the DAT terminal 147 to H level (1409). It is shown in the host equipment 220 that security processing completed MMC110 by this.

[0096]Drawing 15 is a figure showing an example of the signal wave form of the security processing 1407 in drawing 14. In drawing 15, the direction of time is taken on the right from the left. The top lines are the contents of access to the flash memory chip 130. The signal observed toward a lower line with the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the line of the second line is expressed from a top. A lateral dashed line expresses the standard (L level) of each signal. 1501 expresses the signal wave form of the cold reset shown in drawing 3, and 1504 expresses the signal wave form of the warm reset shown in drawing 4, 1502 and 1505 express the signal wave form of the configuration shown in drawing 11 (or drawing 12), 1503, and 1506 and 1507 express the signal wave form of the IC card command processing shown in drawing 5, and 1508 expresses the signal wave form of the deactivation shown in drawing 6. That the signal wave form shown in drawing 15 in the external terminal of the IC card chip 150 is observed, The flow chart of drawing 13 1301, 1302, 1303, 1306, 1307, 1308, 1309, 1310, 1311, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1304, 1306, 1308, 1309, It is a time of changing in order of 1310, 1311, 1314, 1315, and 1316.

[0097]Drawing 15 is referred to and access (read/write 1408) to the flash memory chip 130 by CPU121 under execution of the security processing 1407 of drawing 14 is explained. The security processing buffer space 2114 in drawing 21 is used for this access. The leads 1509, 1511, and 1512, It

is access which leads data required in order to build the IC card command which transmits to the IC card chip 150 in the security command processings 1503, 1506, and 1507, respectively from the flash memory chip 130. The light 1510 is access which carries out the light of the calculation result which the IC card chip 150 outputted in the security command processing 1503 to the flash memory chip 130. The light 1513 is access which summarizes the calculation result which the IC card chip 150 outputted in the security command processings 1506 and 1507 to the flash memory chip 130, and carries out a light. The leads 1509, 1511, and 1512 can be made to overlap access to the security command processings 1503 and 1506 and the IC card chip 150 before 1507, respectively. The lights 1510 and 1513 can be made to overlap access to the security command processing 1503 and the IC card chip 150 after 1507, respectively. These overlap is effective for shortening of the overall processing time of security processing. When the light unit of the flash memory chip 130 is large, the light of two or more calculation results can be collectively carried out like the light 1513. This reduces the number of times of a light to the flash memory chip 130, and it is effective in delaying degradation of the flash memory chip 130. The contents which carry out a light to the flash memory chip 130 in the lights 1510 and 1513 may be a security processing result which it is not limited to the calculation result itself which the IC card chip 150 outputted, but is returned to the host equipment 220 at Step 715 of drawing 7, or its part. In this case, Step 714 of drawing 7 or its part will be performed in Step 712.

[0098]In a process (Steps 713-715 of drawing 7) after, as for drawing 16, the host equipment 220 publishes a security processing result read command to MMC110 until MMC110 outputs a security processing result, They are a signal wave form of the external terminal of MMC110, and the figure which expressed briefly access to the flash memory chip 130 by CPU121. In drawing 16, the direction of time is taken on the right from the left. The top lines are the contents of access to the flash memory chip 130. The signal observed toward a lower line with the VCC1 terminal 144, the CMD terminal 142, the CLK1 terminal 145, and the DAT terminal 147 from the line of the second line is expressed from a top. A lateral dashed line expresses the standard (L level) of each signal.

[0099]A process after the host equipment 220 publishes a security processing result read command to MMC110 with reference to drawing 16 until MMC110 outputs a security processing result is explained. First, the host equipment 220 transmits a security processing result read command to the CMD terminal 142 (1601). Next, the host equipment 220 receives the response of a security processing result read command from the CMD terminal 142 (1602). This response tells that MMC110 received the command to the host equipment 220, and is not a security processing result. Next, MMC110 sets the DAT terminal 147 to L level (1603). It is shown in the host equipment 220 that MMC110 is a busy state by this. Next, CPU121 leads the calculation result which the IC card chip 150 outputted from the security processing buffer space (2114 of drawing 21) of the flash memory chip 130 (1604). CPU121 builds a security processing result based on this, and MMC110 outputs a security processing result to the DAT terminal 147 (1605). When Step 714 of drawing 7 or its part is performed in Step 712, at Step 1604, a security processing result or its part is led from the security processing buffer space (2114 of drawing 21) of the flash memory chip 130. Step 1604 is unnecessary, when building a security processing result without using the security processing buffer space (2114 of drawing 21) of the flash memory chip 130.

[0100]When a problem occurs in MMC110 which its user before providing the user of a security system with MMC110 owns, the manufacturer and administrator of MMC110, It is necessary to write various initial datas in the IC card chip 150 built in MMC110, or to test the IC card chip 150. In order to improve the convenience of these operations by the manufacturer and administrator of MMC110, MMC110 has an interface function which assigns the external terminal of the IC card chip 150 to the MMC external terminal 140. Thereby, the access signal to the IC card chip 150 as shown by drawing 3 - drawing 6 transmits and receives directly from the MMC external terminal 140. Such operational mode of MMC110 is hereafter called interface direct communication mode in distinction from the operational mode based on MMC specification.

[0101]Interface direct communication mode is explained in detail. Drawing 17 is a figure showing an example correspondence-related when assigning the external terminal of the IC card chip 150 to the MMC external terminal 140. In this example, assign the RST terminal 152 to the CS terminal 141, and the GND2 terminal 155 is assigned to the GND1 terminals 143 and 146, The VCC2 terminal 151 is assigned to the VCC1 terminal 144, the CLK2 terminal 153 is assigned to the CLK1 terminal 145, and the I/O terminal 157 is assigned to the DAT terminal 147. At this time, as for the CS terminal 141 and the CLK1 terminal 145, an input terminal and the DAT terminal 147 function as input/output terminals.

[0102]Operational mode can be moved to interface direct communication mode, or MMC110 can return it to the operational mode based on MMC specification from interface direct communication mode, if a specific memory card command is received. The memory card command which returns hereafter the memory card command which moves operational mode to interface direct communication mode to a direct communication-ized command, and returns operational mode to the usual state from interface direct communication mode is called a return command. With reference to drawing 1, the MMCI/F control circuit 123, If it is connected with the VCC2 control circuit 126, the CLK2 control circuit 127, and the IC card I/F control circuit 128 and MMC110 receives a direct communication-ized command from the host equipment 220, terminal allotment shown by drawing 17 with directions of CPU121 will be performed. If MMC110 receives a return command from the host equipment 220, the terminal allotment shown by drawing 17 with directions of CPU121 will be canceled, and MMC110 will return to the operational mode based on MMC specification.
[0103]In interface direct communication mode, since the direct access of the host equipment 220 can be carried out to the IC card chip 150, it is necessary to make to be able to use interface direct communication mode from a viewpoint of security only into the limited person. So, transmission of the password which is not known by the general user is needed for issue of a direct communication-ized command. Unless a right password is entered, interface direct communication mode cannot be used.
[0104]The host equipment 220 moves drawing 18 from the operational mode based on MMC specification in the operational mode of MMC110 to interface direct communication mode, It is a flow chart which shows procedure until it carries out direct access to the IC card chip 150 and returns the operational mode of MMC110 to the operational mode again based on MultiMediaCard specification after that. The host equipment 220 starts processing (1801) and publishes a direct communication-ized command to MMC110 first (1802). The password transmitted by the direct communication-ized command checks MMC110 in the right (1803). Processing will be ended, if right and wrong [move and] to Step 1804 (1810). In Step 1804, CPU121 carries out cold reset of the IC card chip 150. And terminal allotment shown by drawing 17 is performed, and an interface is direct-communication-ized (1805). From this time, direct access of the host equipment 220 is carried out to the IC card chip 150 (1806). The host equipment 220 ends the direct access to the IC card chip 150, and when returning the operational mode of MMC110 to the operational mode again based on MMC specification, a return command is published to MMC110 (1807). Then, CPU121 cancels the terminal allotment shown by drawing 17, and MMC110 returns to the operational mode based on MMC specification (1808). And CPU121 deactivates the IC card chip 150 (1809). Above, processing is ended (1810).
[0105]Drawing 19 is the figure which expressed briefly the signal wave form of the external terminal of MMC110 and the IC card chip 150 in the process of Steps 1801-1806 of drawing 18. In drawing 19, the direction of time is taken on the right from the left. The signal observed toward a lower line with the VCC1 terminal 144, the CMD terminal 142, the CLK1 terminal 145, the DAT terminal 147, the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the upper line is expressed. A lateral dashed line expresses the standard (L level) of each signal. 1905 shows the signal wave form of the cold reset of drawing 3. The mode transition time 1906 expresses the time from which operational mode moves to interface direct communication mode.
[0106]With reference to drawing 19, the process which the host equipment 220 moves the operational mode of MMC110 from the operational mode based on MMC specification to interface direct communication mode, and carries out direct access to the IC card chip 150 is explained. 3V (standard voltage of the VCC2 terminal 151) is supplied to the VCC1 terminal 144 of MMC110. If the host equipment 220 inputs a direct communication-ized command into the CMD terminal 142 (1901), the response of a direct communication-ized command will be outputted from the CMD terminal 142 (1902). This response tells that MMC110 received the command to the host equipment 220. Next, the host equipment 220 enters a password into the DAT terminal 147 (1903). MMC110 outputs L level to the DAT terminal 147 after password input (1904), and it is shown in the host equipment 220 that it is a busy state. Between busy states, CPU121 carries out cold reset of the IC card chip 150 (1905). And in the mode transition time 1906, operational mode is moved to interface direct communication mode. At this time, the DAT terminal 147 will be from L level in a high impedance state. Thereby, the host equipment 220 can know release of a busy state. From this time, direct access of the host equipment 220 is carried out to the IC card chip 150. For example, if a clock is supplied to the CLK1 terminal 145 (1907), the clock will be supplied to the CLK2 terminal 153 (1908). If an IC card command is transmitted to the DAT terminal 147 (1909), the IC card command will be transmitted to the I/O terminal 157 (1910).
[0107]Drawing 20 is the figure which expressed briefly the signal wave form of the external terminal of

MMC110 and the IC card chip 150 in the process of Steps 1807-1810 of drawing 18. In drawing 20, the direction of time is taken on the right from the left. The signal observed toward a lower line with the VCC1 terminal 144, the CMD terminal 142, the CLK1 terminal 145, the DAT terminal 147, the VCC2 terminal 151, the RST terminal 152, the CLK2 terminal 153, and the I/O terminal 157 from the upper line is expressed. A lateral dashed line expresses the standard (L level) of each signal. The mode return time 2003 expresses the time when operational mode returns from interface direct communication mode to the operational mode based on MMC specification. 2004 shows the signal wave form of deactivation of drawing 6.

[0108]With reference to drawing 20, the host equipment 220 explains the process in which the operational mode of MMC110 is returned to the operational mode based on MMC specification from interface direct communication mode. 3V (standard voltage of the VCC2 terminal 151) is supplied to the VCC1 terminal 144 of MMC110. If the host equipment 220 inputs a return command into the CMD terminal 142 (2001), the response of a return command will be outputted from the CMD terminal 142 (2002). This response tells that MMC110 received the command to the host equipment 220. And in the mode return time 2003, MMC110 outputs L level to the DAT terminal 147, shows that it is a busy state to the host equipment 220, and returns operational mode to the operational mode based on MMC specification simultaneously with it. Between busy states, CPU121 deactivates the IC card chip 150 (2004). And it is shown in the host equipment 220 that MMC110 made the DAT terminal 147 the high impedance state (2005), and processing of the return command completed it. The host equipment 220 cannot carry out direct access to the IC card chip 150 after this. When the host equipment 220 transmits a certain memory card command to the CMD terminal 142, supplying a clock to the CLK1 terminal 145, the clock signal (2006) does not get across to the IC card chip 150. Although the clock signal which the host equipment 220 supplies to the CLK1 terminal 145 in 2001 and 2002 gets across also to the CLK2 terminal 153 of the IC card chip 150, Since the DAT terminal 147 is a high impedance state, the IC card chip 150 does not recognize an IC card command accidentally.

[0109]In drawing 21, the information which shows the advancing situation of the security processing by the IC card chip 150 is stored in the security processing status areas 2116. CPU121 can update this information during execution of security processing. For example, if CPU121 leads and refers to this information at the time of resumption of current supply when the current supply of MMC110 stops in the middle of security processing, it can resume from the stage which interrupted security processing.

[0110]MMC110 in this invention can aim at improvement in the speed of processing, and shortening of processing time by processing simultaneously with two or more chips among three, the controller chip 120, the flash memory chip 130, and the IC card chip 150. Operation of the parallel processing which can be hereafter performed by MMC110 which applied this invention is explained. Drawing 27 is the flow chart which showed the procedure of the data read processing which can be processed in parallel. Host equipment 220 and MMC110 ends initial setting so that command processing after powering on can be performed, and it has become the waiting state 2701 and the waiting state 2719 respectively. If the host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (2702), MMC110 will receive the first command (2709) and will return the first response (2710). Here, a response is data which MMC110 which received the command returns to the host equipment 220. Since it is data which will be returned if a command is only received, it does not mean that the execution that whose a response is returned it is a command was completed.

[0111]The controller chip 120 of MMC110 interprets the first command, emits control instruction to the flash memory chip 130 or the IC card chip 150, and starts the first processing (2715). The host equipment 220 will transmit the second command, if the first response is received (2704). Performing the first processing, from the host equipment 220, the controller chip 120 of MMC110 receives the second command, and returns (2705) and the second response (2712). The controller chip 120 interprets the second command and performs the second processing (2713).

[0112]The second command judges and sets up the command which can be processed simultaneously with the first command beforehand with the host equipment 220. The judgment of the command which can be processed simultaneously may be performed by the controller chip 120. Hereafter, the command which can be executed simultaneously is called the command in which parallel execution is possible. It is a command which accesses the chip with which the command which accesses the flash memory chip 130 differed from the command etc. which access the IC card chip 150 as a command in which parallel execution is possible, for example. For example, the command which performs processing which the command which reads music data from the flash memory chip 130 is equivalent to the first command, and decrypts the enciphered data is equivalent to the second command.

[0113]After the first processing is completed, the controller chip 120 transmits the first data to the host equipment 220 (2716). Then, the second data is transmitted (2714). With the controller chip 120 of MMC110, and the host interface 223 of the host equipment 220, distinction of the first data and the second data adds identification information to data, and a management judgment is made. Hereafter, the data which added identification information is called data.
[0114]When the host equipment 220 publishes the command in which parallel execution is possible as the third command while transmission of the first processing was completed and carrying out the second processing, the controller chip 120 interprets the command of the third command in accordance with execution of the second processing, and performs the third processing (2717). If the first command is a command which requires mass data (stream data etc.), the third processing will be performed (2717) and waiting and the third data will be transmitted for the end of transmission of the second data (2718). After that, if there is no command, MMC110 will be from the host equipment 220 in a waiting state (2719). The host equipment 220 will be in a waiting state, if required data is received from MMC110 (2701).
[0115]Drawing 28 is a command when carrying out parallel processing of the read command, data flow, and a figure showing processing along with a time-axis. The host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (2702). The controller chip 120 interprets the first command and gives control instruction to the flash memory chip 130. During the first processing (2715), the host equipment 220 transmits to the CMD terminal 142 of MMC110 by making into the second command the command in which parallel execution is possible (2704). The controller chip 120 interprets the second command, gives control instruction to the IC card chip 150, and performs the second processing (2713). MMC110 transmits data in order like the first data 2803 and the second data 2804. When the host equipment 220 publishes the command which accesses the flash memory chip 130 as the third command during the second processing (2713) (2801), the controller chip 120 gives control instruction to a flash memory chip. MMC110 waits for the end of transmission of the second data 2804, and transmits the third data 2805. The command to which the first command sends large capacity data (stream data etc.) may be sufficient as the third data 2805. In that case, there may not be issue (2801) of the third command and a signal of the third response (2802). The flash memory chip 130 may be the IC card chip 150 as an object with which the controller chip 120 takes out control instruction, and the above contents of processing may be when reverse like the flash memory chip 130 in the IC card chip 150.
[0116]Drawing 29 is a figure showing the flow of the data write processing which can be processed in parallel. Host equipment 220 and MMC110 ends initial setting so that command processing after powering on can be performed, and it has become the waiting state 2901 and the waiting state 2910 respectively. The host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (2902). MMC110 receives the first command (2911), returns the first response (2912), receives the first data simultaneously (2913), and is prevented from transmitting data from the data terminal 147. This is called a busy state below. After MMC110 receives data from the host equipment 220, it is not necessary to make it into a busy state. Step 2913 which receives the first data may not be simultaneous with the first response (2912).
[0117]The host equipment 220 receives the first response (2903), and transmits to the CMD terminal 142 by making into the second command the command in which parallel execution is possible (2904). If MMC110 receives the second command (2914) and the first data is received from the host equipment 220 (2913), it will receive, it transmits the second response (2915), and starts the second processing (2920). If it is a data busy state, it will carry out to the address selection performed by the second processing, and will wait for the second data transfer. The second processing may continue the processing in which not only an address selection chisel but execution is possible. The host equipment 220 receives the second response (2905), waits for release of a busy state, and transmits the second data (2907). When the first command transmits large capacity data (stream data etc.), MMC110 starts the third processing during the second processing (2920) (2921), and waits for the third data transfer (2908). If a busy state is canceled, MMC110 will receive the third data (2918) and will continue the third processing. After that, if there is no command, MMC110 will be from the host equipment 220 in a waiting state (2910). The host equipment 220 will be in a waiting state, if it finishes transmitting data required for MMC110 (2901).
[0118]Drawing 30 is a figure showing a command when carrying out parallel processing of the write command, data flow, and processing along with a time-axis. The host equipment 220 transmits the first command that carries out the light of the data to the flash memory chip 130 to the CMD terminal 142 of MMC110 (2902), and transmits waiting (2903) and the first data for the first response (3003).

MMC110 will transmit the first response, if the first command is received (2903), it will give control instruction to the flash memory chip 130 (the first processing 2916), and will be in a busy state. It is not necessary to make it a busy state here. The host equipment 220 transmits the second command that transmits data to the IC card chip 150 as a command in which parallel execution is possible, transmitting the first data 3003 (2904). The host equipment 220 receives the second response (2905), waits for release of a busy state, and transmits the second data 3004. The controller chip 120 gives control instruction to the IC card chip 150, starts the second processing, and waits for the second data 3004. The host equipment 220 will transmit the second data 3004 transmitted to the IC card chip 150, if a busy state is canceled.

[0119]MMC110 will be in a busy state, if the second data is received (2917). The issue of the third command, then (3001) which the host equipment 220 accesses at the flash memory chip 120 while the IC card chip 150 processes (2920 in the second processing), MMC110 transmits the third response (3002), and the controller chip 120 gives control instruction to a flash memory chip, and starts the third processing (2921). The host equipment 220 waits for release of a busy state, and transmits the third data (3005). When the first command that accesses the flash memory chip 130 transmits large capacity data (stream data etc.), Waiting for release of the busy state under processing of the IC card chip 150 (the second processing 2920), the host equipment 220 transmits the third data 3005 to the flash memory chip 130. MMC110 receives the third data 3005, gives control instruction to the flash memory chip 130, and performs the third processing.

[0120]The flash memory chip 130 may be the IC card chip 150 as an object with which the controller chip 120 takes out control instruction, and the above contents of processing may be when reverse like the flash memory chip 130 in the IC card chip 150.

[0121]Drawing 31 is a figure showing processing of a command in which the data which can be processed in parallel is not transmitted. Host equipment 220 and MMC110 ends initial setting so that command processing after powering on can be performed, and it has become the waiting state 3101 and the waiting state 3110 respectively. The host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (3102). MMC110 receives the first command (3111), transmits the first response to the host equipment 220 (3112), and starts the first processing (3116). The host equipment 220 will transmit the command in which parallel execution is possible as the second command, if the MMC110 to first response is received (3103) (3104). If the second command is received (3113), MMC110 will transmit the second response to the host equipment 220 (3114), and will perform the second processing (3115). After the post-processing finishes, the host equipment 220 will be in the waiting state 3101, and MMC110 will be in the state of the waiting state 3110.

[0122]Drawing 32 is a figure showing processing in case the command which does not transmit the data which can be processed in parallel performs along with a time-axis. The host equipment 220 transmits the first command that accesses the flash memory chip 130 which does not perform data transfer for the CMD terminal 142 of MMC110 (3102). MMC110 receives the first command (3111), and the controller chip 120 gives control instruction to the flash memory chip 130, and starts the first processing (3114). The host equipment 220 receives the first response (3103), and transmits the second command that accesses the IC card chip 150 which does not perform data transfer for the CMD terminal 142 of MMC10 (3104). MMC110 receives the second command (3113), and the controller chip 120 gives control instruction to the IC card chip 150, and performs the second processing (3115). The host equipment 220 transmits to the CMD terminal 142 of MMC110 by making into the third command the command which can be executed only by the internal processing of the controller chip 120 (3201). MMC110 receives the third command and performs the third processing (3203). At this time, the first processing and the second processing may be [be / it] under execution.

[0123]In the above processing, 2 processings of a throat may be sufficient as the first command and the second command among the processing which accesses the flash memory chip 130, the processing which accesses the IC card chip 150, and 3 processings of the internal processing of the controller chip 120. The command which performs same processing by the command which a continuation command can execute only by the internal processing of the controller chip 120 may validate only the command published later.

[0124]Drawing 33 is a figure showing the flow of processing of a command without the data read processing and data transfer which can be processed in parallel. Host equipment 220 and MMC110 ends initial setting so that command processing after powering on can be performed, and it has become the waiting state 3301 and the waiting state 3310 respectively. The host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (3302). MMC110 receives the first

command (3311), transmits the first response to the host equipment 220 (3312), and starts the first processing (3316). The host equipment 220 receives the first response (3303), and transmits the command in which parallel execution is possible as the second command (3304). MMC110 receives the second command (3313) and returns the second response (3314). The first data is transmitted from the DAT terminal 147 between them (3317), and the second processing is started (3315). The host equipment 220 receives the first data (3306), and receives the second response (3305). The host equipment 220 transmits the third command as a command in which parallel processing is possible (3307). MMC110 receives the third command (3318) and returns the third response (3319). The host equipment 220 carries out the third response reception (3308). MMC110 performs the third processing 3120 and transmits the second data (3321). The host equipment 220 receives the second data (3309). If there is no command executed after that, the host equipment 220 will be in the waiting state 3301, and MMC110 will be in the waiting state 3310.

[0125]Drawing 34 is a figure showing the flow of processing of a command without the data read processing and data transfer which can be processed in parallel along with a time-axis. The host equipment 220 transmits the first command that accesses the flash memory chip 120 to the command terminal 142 of MMC110 (3302). MMC110 returns the first response (3303), and the controller chip 120 gives control instruction to the flash memory chip 130, and starts the first processing (3317). The host equipment 220 transmits the second command that accesses the IC card chip 150 without the data transfer in which parallel execution is possible (3304). MMC110 receives the second command (3313), the second response is returned (3305), and the controller chip 120 gives control instruction to the IC card chip 150, and starts the second processing (3315). MMC110 transmits the first data 3403 to the host equipment 220, after the first processing is completed (3316). The host equipment 220 receives the first data (3306), and transmits the third command that accesses the flash memory chip 130 in which parallel processing is possible (3307). MMC110 returns the third response (3308), and the controller chip 120 performs the third processing (3320), and transmits the second data (3405).

[0126]The flash memory top 130 may be the IC card chip 150, and reverse may be sufficient as the above processing like the flash memory chip 130 in the IC card chip 150. The command which performs internal processing of the controller chip 120 may be sufficient as the command without data transfer. In the case of the command to which the first command transmits large-capacity-data data (stream data etc.), the third command does not need to be published.

[0127]Drawing 35 is a figure showing the flow of processing of a command without the data write processing and data transfer which can be processed in parallel. Host equipment 220 and MMC110 ends initial setting so that command processing after powering on can be performed, and it has become the waiting state 3501 and the waiting state 3510 respectively. The host equipment 220 transmits the first command to the CMD terminal 142 of MMC110 (3502). MMC110 receives the first command (3511) and transmits the first response to the host equipment 220 (3512). The host equipment 220 receives the first response (3503), transmits the command in which parallel execution is possible as the second command (3504), and transmits the first data (3505). MMC110 receives the second command (3513) and returns the second response (3514). The first data will be received and it will be from the DAT terminal 147 in a busy state (3516) in the meantime. If the first data is received (3516), MMC110 will start the first processing (3517) and will start the second processing (3515). The host equipment 220 will transmit the third command, if a busy state is canceled (3507). MMC110 returns the third response (3519). The host equipment 110 will transmit the second data, if the third response is received (3508) (3509). MMC110 will receive the second data (3520), will be in a busy state, and performs the third processing (3521). After processing is completed, the host equipment 220 will be in the waiting state 3501, and MMC110 will be in the waiting state 3510, after processing is completed. By the above processing, MMC110 does not need to be in the busy state after data receiving.

[0128]Drawing 36 is a figure showing the flow of processing of a command without the data write processing and data transfer which can be processed in parallel along with a time-axis. The host equipment 220 transmits the first command that accesses the flash memory chip 130 (3502). MMC110 returns the first response (3503) and carries out it the first data receiving (3505), and the controller chip 120 will give control instruction to the flash memory chip 130, will start the first processing (3517), and will be in a busy state. The host equipment 220 transmits the second command that accesses the IC card chip 150 without the data transfer in which parallel execution is possible (3504). MMC110 receives the second command (3513) and returns the second response (3506). The controller chip 120 starts the second processing of a broth for control instruction to the

IC card chip 150 (3515). The host equipment 220 transmits after that the third command that waits to cancel a busy state and accesses it at the flash memory chip 130 (3507). MMC110 receives the third command (3518), returns the third response (3508) and receives the second data 3509 (3520). The controller chip 120 will give control instruction to the flash memory chip 130, will start the third processing, and will be in a busy state (3521).

[0129]By the above processing, the flash memory chip 130 may become conversely like the flash memory chip 130 in the IC card chip 150 at the IC card chip 150. The internal processing of the controller chip 120 may be sufficient as the processing without data transfer. MMC110 does not need to be in the busy state after data receiving. When the first command is a command which transmits large capacity data (stream data etc.), issue and the third response of the third command are not needed.

[0130]The above operation is composition like the SD card host equipment 2460, SD card 2410 and the memory stick host equipment 2560 which are shown by drawing 24 and drawing 25, and the memory stick 2510, In the case of the concurrent access of the IC card chip 150 in the SD card which lets a controller pass, the flash memory chip 2430 and the IC card chip 150 in a memory stick, and the flash memory chip 2530, it is the same.

[0131]As mentioned above, according to the command from a host, since parallel processing is possible at the flash memory chip 130, the IC card chip 150, and the controller chip 120, improvement in the speed and processing time can be shortened for processing. Therefore, authenticating processing at the time of pulling down money from a bank can be performed, reproducing music data using one MMC110.

[0132]According to the embodiment of this invention, in order not to carry out direct supply of the driving clock of an IC chip from the memory card exterior, processing time of an IC chip cannot be measured correctly, and the execution timing of processing and detection of an order become difficult. An unusual driving clock cannot be supplied but it becomes difficult to generate an arithmetic error. Therefore, the security to a timing analysis, power difference part analysis, and the failure use analysis attacking method improves.

[0133]According to the embodiment of this invention, the control system of an IC chip can be freely set up from the memory card exterior. For example, if the control system which made frequency of the driving clock of an IC chip high if high speed processing was required is set up and low power consumption is required, frequency of the driving clock of an IC chip can be made low, or the control system which stops the driving clock of an IC chip moderately can be set up. Therefore, the security processing which corresponded to the processing performance which a security system requires flexibly is realizable.

[0134]According to the embodiment of this invention, data required for the security processing by an IC chip and the information for managing an IC chip can be held to a flash memory. Therefore, the convenience of security processing can be raised.

[0135]According to the embodiment of this invention, the manufacturer and administrator of MMC can do direct access to the IC chip inside MMC. Therefore, initialization and a maintenance of the IC chip inside MMC are realizable by the same method as the conventional IC card.

[0136]When adding a security function to MMC provided with the flash memory chip according to the embodiment of this invention, by [which received attestation of security evaluator Seki beforehand] carrying out IC card chip addition loading, Since attestation of MMC by security evaluator Seki becomes unnecessary, the development cycle or manufacturing period of MMC is shortened.

[0137]According to the embodiment of this invention, according to the command from host equipment, since parallel processing is possible at a flash memory chip, IC card chip, and the controller chip 120, processing is accelerable.

[0138]

[Effect of the Invention]According to this invention, the effect of improving the security of memory storage is done so. Processing of memory storage can be made high-speed.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－22216
（P2003－22216A）
(43)公開日　平成15年１月24日(2003.1.24)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	２Ｃ００５
	３１０		３１０Ｋ	５Ｂ０１７
Ｂ４２Ｄ　15/10	５０１	Ｂ４２Ｄ　15/10	５０１Ｂ	５Ｂ０３５
	５２１		５２１	
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数８　ＯＬ　（全 36 頁）

(21)出願番号　特願2001－207210(P2001－207210)

(22)出願日　平成13年７月９日(2001.7.9)

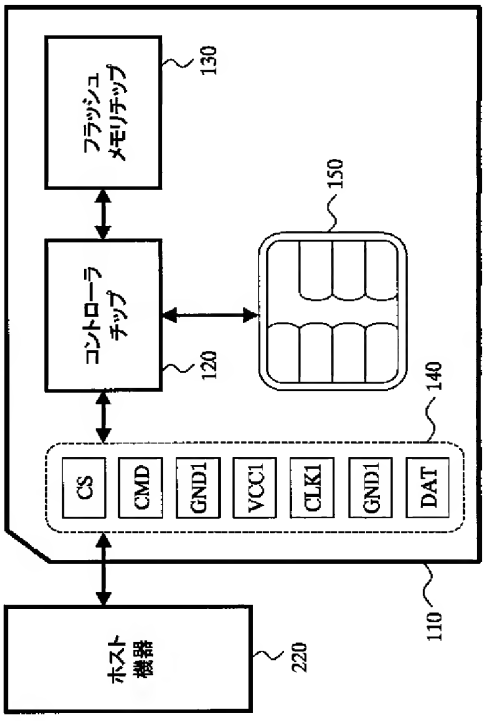
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　幡野　富久
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　戸田　昭憲
神奈川県横浜市戸塚区吉田町292番地　株式会社日立マイクロソフトウェアシステムズ内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　記憶装置

(57)【要約】
【課題】本発明は、マルチメディアカードの処理の高速化を図ることを目的とする。
【解決手段】本発明は、フラッシュメモリチップ１３０と、セキュリティ処理（暗号化や復号化等）を実行可能なＩＣカードチップ１５０と、ホストからの要求に応じて、フラッシュメモリチップ及びＩＣカードチップへのデータの読み書きを制御するコントローラチップ１２０とを備える。さらに、コントローラチップ１２０は、フラッシュメモリチップ１３０とＩＣカードチップ１５０の両方にホストからの要求に応じて同時にアクセスする。

図22



1

【特許請求の範囲】

【請求項１】データを記憶するための記憶装置において、前記データを記憶可能な第１のメモリと、
前記データを記憶可能でかつ前記データのセキュリティ処理を実行可能な第２のメモリと、
ホスト機器からのコマンドに基づいて、前記第１のメモリ又は前記第２のメモリを選択するコントローラとを有し、
前記ホスト機器から前記第１のメモリへのアクセスを実行している間に前記第２のメモリに対する前記ホスト機器からの第２のコマンドを受け付け、前記第２のコマンドに従う処理を実行することを特徴とする記憶装置。

【請求項２】前記コントローラは、前記ホスト機器からのコマンドに前記データのセキュリティ処理に関する情報が含まれていた場合に、前記第２のメモリを選択する請求項１に記載の記憶装置。

【請求項３】前記第２のメモリは、セキュリティ評価機関によって予め認証されたＩＣチップであることを特徴とする請求項１記載の記憶装置。

【請求項４】前記認証済ＩＣチップは、該認証済ＩＣチップへ読み書きされるデータを暗号化又は復号化する手段を有することを特徴とする請求項３記載の記憶装置。

【請求項５】前記第１のメモリは、前記ホスト機器からのデータを記憶する第１の記憶領域と、前記第２のメモリに関するデータを記憶し、前記ホスト機器からのデータの読み出し又は書き込みの少なくとも１つが制限される第２の記憶領域とを有することを特徴とする請求項４記載の記憶装置。

【請求項６】前記コントローラは、前記第２の記憶領域に記憶されたデータを、前記第２のメモリへ転送する手段を有することを特徴とする請求項５記載の記憶装置。

【請求項７】前記コントローラは、前記第２の記憶領域に記憶されたデータに基づいて、前記第２のメモリを制御することを特徴とする請求項６記載の記憶装置。

【請求項８】コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、
前記コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と前記公開鍵に対応する秘密鍵とを記憶し、前記秘密鍵によって前記セッション鍵を復号化することが可能なメモリ付演算処理装置と、
ホストからのコマンドに応じて、前記メモリ付演算処理装置に前記第一のコンテンツに対応する前記セッション鍵の復号化させながら、既に復号化された前記第二のコンテンツに対応する前記セッション鍵によって前記メモリに記憶された前記第二のコンテンツを復号化し、復号化された前記コンテンツを前記ホストへ送信するコントローラとを備えた記憶装置。

【発明の詳細な説明】

【０００１】

2

【発明の属する技術分野】本発明は、セキュリティ機能を搭載した記憶装置、その記憶装置が挿入可能なホスト機器、及びその記憶装置が挿入されたホスト機器に係り、特に、フラッシュメモリチップ及びコントローラを有するメモリカード及びそのメモリカードが挿入可能な装置及びそのそのメモリカードが挿入された端末装置に関する。

【０００２】

【従来の技術】ＩＣカードは、プラスチックカード基板中にＩＣ（集積回路）チップを埋め込んだものであり、その表面にＩＣチップの外部端子を持つ。ＩＣチップの外部端子には、電源端子、クロック端子、データ入出力端子などが含まれる。ＩＣチップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。

【０００３】ＩＣカードは、外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、ＩＣカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ＩＣカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ＩＣカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

【０００４】

【発明が解決しようとする課題】セキュリティシステムにおいて利用されるＩＣカードは、ＩＣカード内部で秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報をＩＣカードの外部にもらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このような外部にもらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分解析、故障利用解析などが知られている。

【０００５】タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを装置に実装する際、暗号の処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要となる処理をスキップしたり分岐処理を行ったりするような最適化が行われることがある。このような最適化を行った場合、暗号処理時間が秘密情報の内容に依存して異なる。そのため、処理時間を見ることで秘密情報の内容を推定できる可能性がある。

【０００６】電力差分解析は、暗号処理を実行している最中に、ＩＣカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

【０００７】故障利用解析は、ＩＣカードの計算誤りを

利用した攻撃法である。ＩＣカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ＩＣカードに攻撃者の望む異常な処理を行わせる。例えば、ＩＣカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合に得られる誤った計算結果と正しい計算結果から秘密情報が取得される可能性がある。

【０００８】したがって、ＩＣカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

【０００９】本発明の目的は、セキュリティを向上した記憶装置を提供することにある。

【００１０】

【課題を解決するための手段】上記課題を解決するため、本発明は、データを記憶するための記憶装置において、データを記憶可能な第１のメモリと、データを記憶可能でかつデータのセキュリティ処理を実行可能な第２のメモリと、ホスト機器からのコマンドに基づいて、第１のメモリ又は第２のメモリを選択するコントローラと有し、ホスト機器から第１のメモリへのアクセスを実行している間に第２のメモリに対するホストからの第２のコマンドを受け付け、第２のコマンドに従う処理を実行する構成とする。

【００１１】又、コントローラは、ホスト機器からのコマンドにデータのセキュリティ処理に関する情報が含まれていた場合に、第２のメモリを選択する構成でも良い。

【００１２】さらに、第２のメモリは、セキュリティ評価機関によって予め認証されたＩＣチップであることも考えられる。

【００１３】また、認証済ＩＣチップは、認証済ＩＣチップへ読み書きされるデータを暗号化又は復号化する手段を有する。

【００１４】また、第１のメモリは、ホスト機器からのデータを記憶する第１の記憶領域と、第２のメモリに関するデータを記憶し、ホスト機器からのデータの読み出し又は書き込みの少なくとも１つが制限される第２の記憶領域とを有する構成とすることもできる。

【００１５】さらに、コントローラは、第２の記憶領域に記憶されたデータを、第２のメモリへ転送する手段を有することもできる。

【００１６】また、コントローラは、第２の記憶領域に記憶されたデータに基づいて、第２のメモリを制御する構成を有しても良い。

【００１７】さらに、本発明の実施形態として、コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と公開鍵に対応する秘密鍵とを記憶し、秘密鍵によってセッション鍵を復号化することが可能なメモリ付演算処理装置と、ホスト機器からのコマンドに応じて、メモリ付演算処理装置に第一のコンテンツに対応するセッション鍵の復号化させながら、既に復号化された第二のコンテンツに対応するセッション鍵によってメモリに記憶された第二のコンテンツを復号化し、復号化された第二のコンテンツをホスト機器へ送信するコントローラとを有する構成とする。

【００１８】

【発明の実施の形態】図２２は、本発明を適用したＭｕｌｔｉＭｅｄｉａＣａｒｄ（ＭｕｌｔｉＭｅｄｉａＣａｒｄは、ＩｎｆｉｎｅｏｎＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成を示した図である。ＭＭＣ１１０は、ＭＭＣ仕様に準拠するのが好ましい。ＭＭＣ１１０は、ＭＭＣ１１０に接続されたホスト機器２２０から発行されたＭＭＣ仕様に準拠したメモリカードコマンドに基づいて、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。

【００１９】ホスト機器２２０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、及び決済端末等が該当する。

【００２０】ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、及びＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は、外部のホスト機器２２０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子等の７つの端子から構成される。コントローラチップ１２０は、ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、及びＩＣカードチップ１５０と接続され、これらを制御するマイコンチップである。

【００２１】ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、ＩＣカードチップ１５０が有する外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、及びグランド端子がある。コントローラチップ１２０は、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器２２０から要求されたセキュリティ処理に必要な演算をおこなう。

【００２２】図２６は、本発明のＩＣカードチップの内部構成を示す図である。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ（マイコン）１５８、データ（プログラムを含む。）を記憶するためのＲＯＭ（Read

Only Memory）１５９、ＲＡＭ（Random Access Memory）１６０、ＥＥＰＲＯＭ（Electrically Erasable Programmable ROM）１６２、暗号／復号に間する処理を行うための暗号コプロセッサ１６３、及び外部とデータを送受信するためのシリアルインターフェース１６１とを備える。これらはバス１６４によって相互に接続される。

【００２３】暗号コプロセッサ１６３は、ホスト機器２２０からのコマンドに応じて、、セキュリティ処理を実行する。尚、暗号コプロセッサ１６３（ハードウェア）の替わりに、プログラム（ソフトウェア）を用いてＣＰＵ１５８がセキュリティ処理を実行してもよい。セキュリティ処理は、例えば、ＩＣカードチップ１５０内の記憶領域にデータが書き込まれるとき、又は、ＩＣカードチップ１５０内の記憶領域からデータが読み出されるときに実行される。

【００２４】フラッシュメモリチップ１３０は、不揮発性の記憶素子を有する。一般的に、ＩＣカードチップ１５０のＥＥＰＲＯＭ１６２の記憶容量は、フラッシュメモリチップ１３０の記憶容量より小さい。但し、ＥＥＰＲＯＭ１６２の記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

【００２５】ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用するのが望ましい。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。本発明においては、ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【００２６】ＭＭＣ１１０は、ＭＭＣ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本実施形態においては、コントローラチップ１２０は、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。

【００２７】ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０と接続されている。

【００２８】コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。本実施形態によれば、ホスト機器２２０からセキュリティ処理を要求されないときには、コントローラチップ１２０がＩＣカードチップ１５０への電源供給やクロック供給を停止することができ、ＭＭＣ１１０の電力消費を削減することができる。

【００２９】電源が供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理を施す必要がある。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始する機能を有する。また、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなう機能を有する。本実施形態によれば、コントローラチップ１２０は、セキュリティ処理を実行するコマンドを受信するまでＩＣカードチップ１５０への電源供給を停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。

【００３０】コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチップ１５０に供給するクロック信号をＭＭＣ１１０内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を有する。本実施形態によれば、ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器２２０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【００３１】図２１は、フラッシュメモリチップ１３０の内部構成を示す図である。フラッシュメモリチップ１

３０は、ホストデータ領域２１１５及び管理領域２１１０とを有する。ホストデータ領域２１１５は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器２２０が論理アドレスを指定してデータを読み書きできる領域である。

【００３２】ホストデータ領域２１１５は、ユーザファイル領域２１３０及びセキュリティ処理アプリケーション領域２１２０とを有する。ユーザファイル領域２１３０は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域２１２０は、ホスト機器２２０がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器２２０のセキュリティ処理アプリケーションによって論理的にユーザアクセス制限がかけられる。ここに格納されるデータとしては、ホスト機器２２０のアプリケーションプログラム、そのアプリケーション専用のデータ、及びセキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）がある。本実施形態によれば、ＭＭＣ１１０が、ホスト機器２２０がセキュリティ処理をおこなう上で使用するデータをホスト機器２２０の代わりに格納するため、ホスト機器２２０にとって利便性が向上する。

【００３３】管理領域２１１０は、コントローラチップ１２０がＩＣカードチップ１５０を管理するための情報を格納する領域である。管理領域２１１０は、ＩＣカード制御パラメータ領域２１１１、ＩＣカード環境設定情報領域２１１２、ＣＬＫ２設定情報領域２１１３、セキュリティ処理バッファ領域２１１４、及びセキュリティ処理ステータス領域２１１６とを有する。２１１１～２１１６の領域の詳細な使用法については後述する。

【００３４】コントローラチップ１２０は、フラッシュメモリチップ１３０の管理領域２１１０のセキュリティ処理バッファ領域２１１４を、ＩＣカードチップ１５０でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器２２０がセキュリティ処理を実行するコマンドによりＭＭＣ１１０にアクセスした際に、ＭＭＣ１１０がホスト機器２２０からＩＣカードチップ１５０に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ１２０は、フラッシュメモリチップ１３０へのアクセスを選択し、受信したデータを十分な容量を持つセキュリティ処理バッファ領域２１１４に一時的に格納する。ＩＣカードチップ１５０に一度に送信できないほどのサイズとは、ＩＣカードコマンドの許容データサイズ（例えば、２５５バイト又は２５６バイト）を超えるサイズである。そして、コントローラチップ１２０はそれをＩＣカードチップ１５０に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ１３０から読み出し、段階的にＩＣカードチップ１５０に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本実施形態によれば、ホスト機器２２０にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

【００３５】セキュリティ処理バッファ領域２１１４を含む管理領域２１１０は、ホスト機器２２０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にホストアクセス制限がかけられている。つまり、管理領域２１１０はホスト機器２２０が直接データを読み書きできない。本実施形態によれば、ホスト機器２２０がセキュリティ処理バッファ領域２１１４の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

【００３６】図２３は、ＭＭＣ１１０を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表した図である。コンテンツプロバイダ２３１０は、ＭＭＣ１１０を所有するユーザにコンテンツ２３１４を販売する業者である。ホスト機器２２０は、この例では、コンテンツプロバイダ２３１０とネットワークなどを介して接続することができる端末機である。ユーザは、ＭＭＣ１１０をホスト機器２２０に接続してコンテンツ２３１４を購入する。以下、その手順を説明する。

【００３７】まず、ホスト機器２２０は、ＭＭＣ１１０に、フラッシュメモリチップ１３０に格納されたユーザ証明書２３２１を読み出すコマンドを発行する。ＭＭＣ１１０のコントローラチップ１２０は、フラッシュメモリチップ１３０のセキュリティ処理アプリケーション領域２１２０に格納されたユーザ証明書２３２１を読み出し、それをホスト機器２２０に送信する。ユーザ証明書２３２１を受信したホスト機器２２０は、それをコンテンツプロバイダ２３１０に送信する。コンテンツプロバイダ２３１０は、ユーザ証明書２３２１につけられたデジタル署名を検証する（２３１１）。検証が成功したならば、コンテンツプロバイダ２３１０は、乱数発生器によりセッション鍵を生成し（２３１２）、それをユーザ証明書２３２１から抽出したユーザ公開鍵によって暗号化する（２３１３）。さらに、コンテンツプロバイダ２３１０は、コンテンツ２３１４をセッション鍵によって暗号化する（２３１５）。コンテンツプロバイダ２３１０は、ステップ２３１３の結果をホスト機器２２０に送信する。

【００３８】ホスト機器２２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するＩＣカー

ドコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、ユーザ秘密鍵２３２２によってステップ２３１３の結果を復号して、セッション鍵を取得する（２３２３）。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。

【００３９】次に、コンテンツプロバイダ２３１０は、ステップ２３１５の結果を、ホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をセッション鍵（ステップ２３２３によって取得した鍵）によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１５の結果をセッション鍵によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、セッション鍵によってステップ２３１５の結果を復号して、コンテンツ２３１４を復元する（２３２４）。コントローラチップ１２０は、このコンテンツ２３１４をＩＣカードチップ１５０から受信し、フラッシュメモリチップ１３０に書きこむ。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。ホスト機器２２０が、コンテンツを無事に受信したことをコンテンツプロバイダ２３１０に伝えると、コンテンツプロバイダ２３１０はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。ユーザは、ホスト機器２２０でＭＭＣ１１０内のフラッシュメモリチップ１３０に格納されたコンテンツ２３１４を読み出して利用することができる。また、フラッシュメモリチップ１３０の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。本実施形態によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をＭＭＣ１１０によって容易に実現できる。コンテンツ料金の決済を、ＩＣカードチップ１５０を利用して行ってもよい。

【００４０】図２４及び図２５は、それぞれ、本発明をＳＤカード（幅２４ミリメートル、長さ３２ミリメートル、厚さ２。１ミリメートルで、９つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。）及びメモリースティック（メモリースティックはソニー株式会社の登録商標である。）に適用したときの内部構成を表した図である。

【００４１】本発明を適用したＳＤカード２４１０は、ＳＤカードコントローラチップ２４２０、フラッシュメモリチップ２４３０、ＳＤカード外部端子２４４０、及びＩＣカードチップ１５０とを有する。本発明を適用したメモリースティック２５１０は、メモリースティックコントローラチップ２５２０、フラッシュメモリチップ２５３０、メモリースティック外部端子２５４０、及びＩＣカードチップ１５０とを有する。

【００４２】フラッシュメモリチップ２４３０及び２５３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＳＤカードコントローラチップ２４２０及びメモリースティックコントローラチップ２５２０は、それぞれＳＤカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

【００４３】ＳＤカード外部端子２４４０は、端からＤａｔａ２端子２４４１、Ｄａｔａ３端子２４４２、Ｃｏｍ端子２４４３、Ｖｓｓ端子２４４４、Ｖｄｄ端子２４４５、Ｃｌｏｃｋ端子２４４６、Ｖｓｓ端子２４４７、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９の順で並ぶ９つの端子を有する。Ｖｄｄ端子２４４５は電源供給端子、Ｖｓｓ端子２４４４及び２４４７はグランド端子、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９、Ｄａｔａ２端子２４４１及びＤａｔａ３端子２４４２はデータ入出力端子、Ｃｏｍ端子２４４３はコマンド入出力端子、Ｃｌｏｃｋ端子２４４６はクロック入力端子である。ＳＤカード２４１０は、外部に接続するＳＤカードホスト機器２４６０とのインタフェース仕様がＭＭＣ１１０と異なるものの、ＭＭＣ外部端子１４０と非常に類似した外部端子を持ち、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００４４】一方、メモリースティック外部端子２５４０は、端からＧｎｄ端子２５４１、ＢＳ端子２５４２、Ｖｃｃ端子２５４３、予約端子Ｒｓｖを１つ飛ばしてＤＩＯ端子２５４４、ＩＮＳ端子２５４５、予約端子Ｒｓｖを１つ飛ばしてＳＣＫ端子２５４６、Ｖｃｃ端子２５４７、Ｇｎｄ端子２５４８の順で並ぶ１０個の端子を有する。Ｖｃｃ端子２５４３及び２５４７は電源供給端子、Ｇｎｄ端子２５４１及び２５４８はグランド端子、ＤＩＯ端子２５４４はコマンドおよびデータ入出力端子、ＳＣＫ端子２５４６はクロック入力端子である。メモリースティック２５１０は、外部に接続するメモリースティックホスト機器２５６０とのインタフェース仕様がＭＭＣ１１０と異なるものの、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００４５】図１は、本発明を適用したＭＭＣ１１０の内部構成を表した図である。また、図２は、図１のＭＭ

Ｃ１１０と接続したホスト機器２２０の構成とその接続状態を表した図である。ホスト機器２２０は、ＶＣＣ１電源２２１、ＣＬＫ１発振器２２２、ホストインタフェース２２３を持つ。

【００４６】ＭＭＣ１１０は、外部のホスト機器２２０と情報交換するためのＭＭＣ外部端子１４０を持つ。ＭＭＣ外部端子１４０は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＧＮＤ１端子１４３及び１４６、ＶＣＣ１端子１４４、ＣＬＫ１端子１４５、ＤＡＴ端子１４７の７つの端子を有する。ＭＭＣ仕様は、ＭＭＣ１１０の動作モードとしてＭＭＣモードとＳＰＩモードという２種類を規定しており、動作モードによってＭＭＣ外部端子１４０の使用法は異なる。本実施例ではＭＭＣモードでの動作の場合について詳細に説明する。

【００４７】ＶＣＣ１端子１４４は、ＶＣＣ１電源２２１と接続されており、ホスト機器２２０がＭＭＣ１１０に電力を供給するための電源端子である。ＧＮＤ１端子１４３および１４６は、ＶＣＣ１電源２２１と接続されており、ＭＭＣ１１０の電気的なグランド端子である。ＧＮＤ１端子１４３とＧＮＤ１端子１４６は、ＭＭＣ１１０内部で電気的に短絡されている。

【００４８】ＣＳ端子１４１は、ホストインタフェース２２３に接続されており、ＳＰＩモードの動作において使用される入力端子である。ホスト機器２２０が、ＭＭＣ１１０にＳＰＩモードでアクセスするときには、ＣＳ端子１４１にＬレベルを入力する。ＭＭＣモードの動作では、ＣＳ端子１４１を使用する必要はない。ＣＭＤ端子１４２は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをＭＭＣ１１０に送信したり、同仕様に準拠したメモリカードレスポンスをＭＭＣ１１０から受信するために使用する入出力端子である。ＤＡＴ端子１４７は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠した形式の入力データをＭＭＣ１１０に送信したり、同仕様に準拠した形式の出力データをＭＭＣ１１０から受信するために使用する入出力端子である。

【００４９】ＣＬＫ１端子１４５は、ＣＬＫ１発振器２２２に接続されており、ＣＬＫ１発振器２２２が生成するクロック信号が入力される端子である。ホスト機器２２０が、ＣＭＤ端子１４２を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、ＤＡＴ端子１４７を通してホストデータを送受信するときに、ＣＬＫ１端子１４５にクロック信号が入力される。ホストインタフェース２２３には、ＣＬＫ１発振器２２２からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、ＣＬＫ１発振器２２２が生成するクロック信号にビット単位で同期して、ホスト機器２２０とＭＭＣ１１０との間を転送される。

【００５０】ＭＭＣ１１０は、コントローラチップ１２０を持つ。コントローラチップ１２０は、ＣＰＵ１２１、フラッシュメモリＩ／Ｆ制御回路１２２、ＭＭＣＩ／Ｆ制御回路１２３、ＣＬＫ０発振器１２４、ＶＣＣ２生成器１２５、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８とを有する。これらの構成要素１２１～１２８は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。ＭＭＣＩ／Ｆ制御回路１２３は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、及びＤＡＴ端子１４７と接続されており、ＭＭＣ１１０がそれらの端子を通してホスト機器２２０と情報交換するためのインタフェースを制御する論理回路である。

【００５１】ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３と接続されており、ＭＭＣＩ／Ｆ制御回路１２３を制御する。ＭＭＣＩ／Ｆ制御回路１２３がＣＭＤ端子１４２を通してホスト機器２２０からメモリカードコマンドを受信すると、ＭＭＣＩ／Ｆ制御回路１２３は、そのコマンドの受信が成功したかどうかの結果をホスト機器２２０に伝えるためＣＭＤ端子１４２を通してホスト機器２２０にレスポンスを送信する。ＣＰＵ１２１は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器２２０とＤＡＴ端子１４７を通してデータの送受信をおこなう必要がある場合、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３へのデータの送出、ＭＭＣＩ／Ｆ制御回路１２３からのデータの取得をおこなう。さらに、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３とホスト機器２２０との間のデータ転送手続きも制御する。例えば、ホスト機器２２０から受信したデータの処理中に、ホスト機器２２０がＭＭＣ１１０への電源供給を停止することがないように、ＣＰＵ１２１はＤＡＴ端子１４７にＬレベルを出力させ、ＭＭＣ１１０がビジー状態であることをホスト機器２２０に伝える。ＣＬＫ０発振器１２４は、ＣＰＵ１２１と接続され、ＣＰＵ１２１を動作させる駆動クロックを供給する。

【００５２】ＭＭＣ１１０は、フラッシュメモリチップ１３０を有する。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ１３０は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。フラッシュメモリチップ１３０は、外部からのフラッシュメモリコマンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリＩ／Ｆ制御回路１２２は、フラッシュメモリチップ１３０にフラッシュメモリコマンドを発行した

り、そのコマンドで入出力するデータを転送するための論理回路である。ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２を制御し、フラッシュメモリチップ１３０にデータのライト機能やリード機能を実行させる。ホスト機器２２０から受信したデータをフラッシュメモリチップ１３０にライトしたり、フラッシュメモリチップ１３０に格納されたデータをホスト機器２２０に送信する必要があるとき、ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２とＭＭＣＩ／Ｆ制御回路１２３の間のデータ転送を制御する。

【００５３】ＭＭＣ１１０は、ＩＣカードチップ１５０を有する。ＩＣカードチップ１５０は、ＩＣカードの基板中に埋め込むことを目的として設計されたＩＣチップであり、ＩＣカードの外部端子規格に準拠した８つの外部端子を有する。このうち６つの端子は、ＩＣカードの外部端子規格により使用法が割り付けられており、残りの２つは将来のための予備端子である。その６つの端子は、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、ＧＮＤ２端子１５５、ＶＰＰ端子１５６、及びＩ／Ｏ端子１５７である。

【００５４】ＩＣカードチップ１５０のグランド端子は、ＭＭＣ外部端子１４０のGND1（グランド端子）１４６に接続される。ＩＣカードチップ１５０のＶＣＣ２端子（電源入力端子）１５１は、コントローラチップ１２０のＶＣＣ２制御回路１２６に接続される。ＩＣカードチップ１５０のＲＳＴ端子（リセット入力端子）１５２とＩ／Ｏ端子（データ入出力端子）１５７は、コントローラチップ１２０のＩＣカードＩ／Ｆ制御回路１２８に接続される。ＩＣカードチップ１５０のＣＬＫ２端子（クロック入力端子）１５３は、コントローラチップ１２０のＣＬＫ２制御回路１２７に接続される。

【００５５】フラッシュメモリチップ１３０のＶＣＣ端子（電源入力端子）は、ＭＭＣ外部端子１４０のＶＣＣ１１４４に接続される。フラッシュメモリチップ１３０のＶＳＳ端子（グランド端子）は、ＭＭＣ外部端子１４０のGND1１４６に接続される。フラッシュメモリチップ１３０のＩ／Ｏ端子（データ入出力端子）とレディ／ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ１２０のフラッシュメモリＩＦ制御回路１２２に接続される。

【００５６】ＶＣＣ２端子１５１は、ＩＣカードチップ１５０に電力を供給するための電源端子である。ＶＣＣ２制御回路１２６は、ＭＯＳ－ＦＥＴ素子を用いたスイッチ回路によりＶＣＣ２端子１５１への電力の供給開始と供給停止を制御する回路である。ＶＣＣ２生成器１２５はＶＣＣ２端子１５１に供給する電圧を発生し、それをＶＣＣ２制御回路１２６に供給する。ＩＣカードの電気信号規格は、ＩＣカードの動作クラスとして、クラスＡとクラスＢを規定している。ＶＣＣ２端子１５１に供給する標準電圧は、クラスＡでは５Ｖ、クラスＢでは３Ｖである。本発明はＩＣカードチップ１５０の動作クラスによらず適用できるが、本実施例ではＩＣカードチップ１５０がクラスＢで動作する場合について詳細に説明する。

【００５７】ＶＰＰ端子１５６は、ＩＣカードチップ１５０がクラスＡで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスＢで動作する時には使用しない。ＧＮＤ２端子１５５は、ＩＣカードチップ１５０の電気的なグランド端子であり、ＧＮＤ１端子１４３、１４６と短絡されている。ＶＣＣ２制御回路１２６はＣＰＵ１２１と接続され、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給の開始と停止を制御することができる。ＩＣカードチップ１５０を使用しないときは、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給を停止することができる。ＭＭＣ１１０は、ＩＣカードチップ１５０への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ＩＣカードチップ１５０の内部状態は、ＩＣカードチップ１５０内部の不揮発性メモリに記憶されたデータを除いて維持されない。

【００５８】ＣＬＫ２端子１５３は、ＩＣカードチップ１５０にクロック信号を入力する端子である。ＣＬＫ２制御回路１２７は、ＣＬＫ２端子１５３にクロックを供給する回路である。ＣＬＫ２制御回路１２７は、ＣＬＫ０発振器１２４から供給されたクロック信号をもとにしてＣＬＫ２端子１５３に供給するクロック信号を生成する。ＣＬＫ２制御回路１２７はＣＰＵ１２１と接続されており、ＣＬＫ２端子１５３へのクロックの供給開始と供給停止をＣＰＵ１２１から制御することができる。ＩＣカードチップ１５０は、自身内部に駆動クロック発振器をもたない。そのため、ＣＬＫ２端子１５３から駆動クロックを供給することによって動作する。ＣＬＫ２制御回路１２７が、ＣＬＫ２端子１５３へのクロック供給を停止すると、ＩＣカードチップ１５０の動作は停止するため、ＩＣカードチップ１５０の消費電力を低下させることができる。この時、ＶＣＣ２端子１５１への電力供給が保たれていれば、ＩＣカードチップ１５０の内部状態は維持される。

【００５９】ここで、ＣＬＫ２端子１５３に供給するクロック信号の周波数をＦ２、ＣＬＫ０発振器１２４から供給されたクロック信号の周波数をＦ０、ＰとＱを正の整数とすると、ＣＬＫ２制御回路１２７は、Ｆ２＝（Ｐ／Ｑ）＊Ｆ０の関係になるようなクロック信号を作成して、これをＣＬＫ２端子１５３に供給する。ＰとＱの値はＣＰＵ１２１により設定できるようになっている。Ｐを大きく設定してＦ２を大きくすると、ＩＣカードチップ１５０の内部処理をより高速に駆動できる。Ｑを大きく設定してＦ２を小さくすると、ＩＣカードチップ１５

０の内部処理はより低速に駆動され、ＩＣカードチップ１５０の消費電力を低下させることができる。ＩＣカードチップ１５０の駆動クロック周波数は、ＩＣカードチップ１５０が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、ＣＬＫ２制御回路１２７は、Ｆ２の値がその許容周波数範囲を外れるようなＰとＱの値を設定させない特徴を持つ。

【００６０】Ｉ／Ｏ端子１５７は、ＩＣカードチップ１５０にＩＣカードコマンドを入力したり、ＩＣカードチップ１５０がＩＣカードレスポンスを出力するときに使用する入出力端子である。ＩＣカードＩ／Ｆ制御回路１２８は、Ｉ／Ｏ端子１５７と接続されており、Ｉ／Ｏ端子１５７を通してＩＣカードコマンドの信号送信やＩＣカードレスポンスの信号受信をおこなう回路である。ＩＣカードＩ／Ｆ制御回路１２８はＣＰＵ１２１に接続されており、ＣＰＵ１２１は、ＩＣカードＩ／Ｆ制御回路１２８によるＩＣカードコマンドやＩＣカードレスポンスの送受信の手続きを制御したり、送信すべきＩＣカードコマンドデータをＩＣカードＩ／Ｆ制御回路１２８に設定したり、受信したＩＣカードレスポンスをＩＣカードＩ／Ｆ制御回路１２８から取得する。ＩＣカードＩ／Ｆ制御回路１２８にはＣＬＫ２制御回路１２７からクロックが供給されており、ＩＣカードコマンドやＩＣカードレスポンスは、ＣＬＫ２端子１５３に供給するクロック信号にビット単位で同期して、Ｉ／Ｏ端子１５７を通して送受信される。また、ＲＳＴ端子１５２は、ＩＣカードチップ１５０をリセットするときにリセット信号を入力する端子である。ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２と接続されており、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にリセット信号を送ることができる。

【００６１】ＩＣカードチップ１５０は、ＩＣカードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。ＩＣカードチップ１５０へのアクセスパターンは４種類であり、図３～図６を用いて各パターンを説明する。図３は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図４は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図５は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信するプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図６は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０を非活性状態にするプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図３～図６において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００６２】図３を参照して、ＩＣカードチップ１５０のコールドリセット操作を説明する。まず、ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２をＬレベルにする（３０１）。次に、ＶＣＣ２制御回路１２６は、ＶＣＣ２端子への電源供給を開始する（３０２）。次に、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（３０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚ（プルアップされた状態）にする（３０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（３０５）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（３０６）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（３０７）。これで、コールドリセットの操作が完了する。なお、ステップ３０７は消費電力を低下させるための工夫であり、省略してもよい。

【００６３】図４を参照して、ＩＣカードチップ１５０のウォームリセット操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（４０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（４０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（４０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（４０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（４０５）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（４０６）。これで、ウォームリセットの操作が完了する。なお、ステップ４０６は消費電力を低下させるための工夫であり、省略してもよい。

【００６４】図５を参照して、ＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（５０１）。なお、クロックがすでに供給されている場合、ステップ５０１は不要である。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７にコマンドデータの送信を開始する（５０２）。コマンドデータの送信が終了したら、ＩＣ

カードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（５０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるレスポンスデータの受信を開始する（５０４）。レスポンスデータの受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（５０５）。これで、ＩＣカードコマンド送信とＩＣカードレスポンス受信の操作が完了する。なお、ステップ５０５は、消費電力を低下させるための工夫であり、省略してもよい。

【００６５】図６を参照して、ＩＣカードチップ１５０を非活性化する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３をLレベルにする（６０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（６０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７をLレベルにする（６０３）。最後に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を停止する（６０４）。これで、非活性化の操作が完了する。

【００６６】ＩＣカードチップ１５０は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ＩＣカードチップ１５０は、ＣＰＵ１２１との間でＩＣカードコマンドやＩＣカードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送出、記憶されている情報の変更などをおこなう。ＣＰＵ１２１は、ＩＣカードチップ１５０を利用してセキュリティ処理を実行することができる。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、ＶＣＣ２制御回路１２６を通してＩＣカードチップ１５０への電源供給を制御したり、またはＣＬＫ２制御回路１２７を通してＩＣカードチップ１５０へのクロック供給を制御したり、またはＩＣカードＩ／Ｆ制御回路１２８を通してＩＣカードチップ１５０にＩＣカードコマンドを送信する。これにより、ＣＰＵ１２１は、ＩＣカードチップ１５０を利用して、ホスト機器２２０が要求するセキュリティ処理を実行する。ＣＰＵ１２１は、特定のメモリカードコマンドの受信を契機に、ＩＣカードチップ１５０に対する電源供給制御、クロック供給制御、ＩＣカードコマンド送信、ＩＣカードレスポンス受信を複数組み合わせて操作することによって、セキュリティ処理を実行してもよい。また、ＣＰＵ１２１は、ホスト機器２２０がＭＭＣ１１０へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ＩＣカードチップ１５０が出力するＩＣカードレスポンスをベースにして構成され、ＭＭＣ１１０内に保持される。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、セキュリティ処理の結果をホスト機器２２０に送信する。

【００６７】図７は、ホスト機器２２０がＭＭＣ１１０にアクセスするときのフローチャートを表したものである。まず、ホスト機器２２０はＭＭＣ１１０を活性化するためにＶＣＣ１端子１４４に電源供給を開始する（７０１）。これを契機として、ＭＭＣ１１０は、第１次ＩＣカード初期化処理を実行する（７０２）。第１次ＩＣカード初期化処理の詳細は後述する。次に、ホスト機器２２０はＭＭＣ１１０を初期化するためにＣＭＤ端子１４２を通してＭＭＣ１１０の初期化コマンドを送信する（７０３）。この初期化コマンドはＭＭＣ仕様に準拠したものであり、複数種類ある。ホスト機器２２０は、ＭＭＣ１１０を初期化するために、複数の初期化コマンドを送信する場合がある。ＭＭＣ１１０が初期化コマンドを受信すると、ＭＭＣ１１０はそれを処理する（７０４）。これを契機として、ＭＭＣ１１０は、第２次ＩＣカード初期化処理を実行する（７０５）。第２次ＩＣカード初期化処理の詳細は後述する。

【００６８】ホスト機器２２０は、ＭＭＣ１１０の初期化コマンドに対するメモリカードレスポンスを、ＣＭＤ端子１４２を通して受信し、そのメモリカードレスポンスの内容からＭＭＣ１１０の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう（７０３）。ＭＭＣ１１０の初期化が完了したならば、ホスト機器２２０は、ＭＭＣ仕様に準拠した標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド（ＩＣカードチップ１５０へアクセスするためのコマンド）の送信を待機する状態に移る（７０７）。この待機状態では、ホスト機器２２０は標準メモリカードコマンドを送信することができる（７０８）。ＭＭＣ１１０が標準メモリカードコマンドを受信したら、ＭＭＣ１１０はそれを処理する（７０９）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理要求ライトコマンドを送信することもできる（７１０）。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。

【００６９】ＭＭＣ１１０がセキュリティ処理要求ライトコマンドを受信したら、ＣＰＵ１２１は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をＩＣカードコマンドの形式で記述する（７１１）。即ち、ＣＰＵ１２１は、予め定められたルールに従って、ホスト機器２３０からの標準メモリカードコマンドを、ＩＣカードチップ１５０が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られ

たＩＣカードコマンドをＩＣカードチップ１５０に発行するなどして、要求されたセキュリティ処理を実行する（７１２）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理結果リードコマンドを送信することもできる（７１３）。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０によるセキュリティ処理の実行結果を知るために処理結果を受信するメモリカードコマンドである。

【００７０】ＭＭＣ１１０がセキュリティ処理結果リードコマンドを受信したら、ＣＰＵ１２１は、ＩＣカードチップ１５０から受信したＩＣカードレスポンスをベースに、ホスト機器２２０に送信すべきセキュリティ処理結果を構築する（７１４）。そして、ホスト機器２２０は、ＭＭＣ１１０からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。なお、ステップ７１４は、ステップ７１２の中でおこなってもよい。

【００７１】図７において、ステップ７０２およびステップ７０５で実行する第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＭＭＣ１１０内でセキュリティ処理を実行するのに備えて、ＣＰＵ１２１がＩＣカードチップ１５０に対してアクセスする処理である。具体的には、ＩＣカードチップ１５０の活性化や非活性化、ＩＣカードチップ１５０のリセット、ＩＣカードチップ１５０の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報（例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など）をＩＣカードチップ１５０から読み出したり、あるいはＩＣカードチップ１５０に書き込んだりすることを意味する。

【００７２】ＩＣカードチップ１５０の環境設定は、ＩＣカードチップ１５０にＩＣカードコマンドをＮ個（Ｎは正の整数）発行することによっておこなう。例えば、セッション鍵が３個必要ならば、ＩＣカードコマンドを３回発行し、セッション鍵が２個必要ならば、ＩＣカードコマンドを２回発行する。Ｎ個のＩＣカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Ｎの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するＩＣカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するＩＣカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

【００７３】ＣＰＵ１２１は、ＩＣカードチップ１５０の環境設定の内容を自由に変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれを変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、ＣＰＵ１２１は、環境設定の内容を示した情報をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からその情報をリードして使用することもできる。この情報は、図２１においてＩＣカード環境設定情報２１１２として示されている。これにより、ＭＭＣ１１０が非活性化されてもその情報を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００７４】第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＩＣカード制御パラメータＡ、Ｂ、Ｃに設定された値に基づいておこなわれる。また、ＣＰＵ１２１は、ステップ７１２で実行するセキュリティ処理において、ＩＣカード制御パラメータＤに設定された値に基づいてＩＣカードチップ１５０の活性化や非活性化を制御する。

【００７５】図８は、ＩＣカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータＡは、ＭＭＣ１１０に電源が供給されたときに実行される第１次ＩＣカード初期化処理に関するパラメータである。Ａ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ａ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットする。Ａ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ａ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ａ＝０またはＡ＝３のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０が非活性状態となる。Ａ＝１またはＡ＝２のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０は活性状態となる。

【００７６】次に、パラメータＢとＣは、ＭＭＣ１１０がＭＭＣ初期化コマンドを処理したときに実行される第２次ＩＣカード初期化処理に関するパラメータである。Ｂ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ｂ＝１かつＣ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセット（コールドリセットまたはウォームリセット）する。Ｂ＝１かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝１かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカ

ードチップ１５０を非活性化する。Ｂ＝２かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝２かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなった後にＩＣカードチップ１５０を非活性化する。Ｂ＝３のときは、ＩＣカードチップ１５０が活性状態ならば、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

【００７７】最後に、パラメータＤは、ホスト機器２２０から要求されたセキュリティ処理を実行したあとに、ＩＣカードチップ１５０を非活性化するか否かを示すパラメータである。Ｄ＝０のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化せず、活性状態に保つ。Ｄ＝１のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

【００７８】ＣＰＵ１２１は、ＩＣカード制御パラメータＡ、Ｂ、Ｃ、Ｄの設定値を変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＩＣカード制御パラメータ２１１１として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００７９】図９は、第１次ＩＣカード初期化処理の手順を示すフローチャートである。初期化処理を開始する（９０１）と、まず、ＩＣカード制御パラメータＡが０かチェックする（９０２）。Ａ＝０ならばそのまま初期化処理は終了する（９０８）。Ａ＝０でないならばＩＣカードチップ１５０をコールドリセットする（９０３）。次に、ＩＣカード制御パラメータＡが１かチェックする（９０４）。Ａ＝１ならば初期化処理は終了する（９０８）。Ａ＝１でないならばＩＣカードチップ１５０の環境設定をおこなう（９０５）。次に、ＩＣカード制御パラメータＡが２かチェックする（９０６）。Ａ＝２ならば初期化処理は終了する（９０８）。Ａ＝２でないならばＩＣカードチップ１５０を非活性化する（９０７）。そして、初期化処理は終了する（９０８）。

【００８０】図１０は、第２次ＩＣカード初期化処理の手順を示すフローチャートである。初期化処理を開始する（１００１）と、まず、ＩＣカード制御パラメータＢが０かチェックする（１００２）。Ｂ＝０ならばそのまま初期化処理は終了する（１０１３）。Ｂ＝０でないならばＢ＝１かチェックする（１００３）。Ｂ＝１ならばＩＣカード制御パラメータＡが０または３かチェックする（１００４）。Ａが０または３ならば、ＩＣカードチップ１５０をコールドリセットし（１００５）、ステップ１００７に移る。Ａが１または２ならば、ＩＣカードチップ１５０をウォームリセットし（１００６）、ステップ１００７に移る。ステップ１００７では、ＩＣカード制御パラメータＣが１かチェックする。Ｃ＝１ならば初期化処理は終了する（１０１３）。Ｃ＝１でないならばステップ１００９に移る。ステップ１００３においてＢ＝１でないならば、Ｂが２かチェックする（１００８）。Ｂ＝２ならばステップ１００９に移る。Ｂ＝２でないならば、ＩＣカード制御パラメータＡが０または３かチェックする（１０１１）。Ａが０または３ならば初期化処理を終了する（１０１３）。Ａが１または２ならば、ステップ１０１２に移る。ステップ１００９ではＩＣカードチップ１５０の環境設定をおこなう。そして、ＩＣカード制御パラメータＣが２かチェックする（１０１０）。Ｃ＝２ならば初期化処理を終了する（１０１３）。Ｃ＝２でないならばステップ１０１２に移る。ステップ１０１２ではＩＣカードチップ１５０を非活性化する。そして、初期化処理を終了する（１０１３）。

【００８１】図１１は、ＩＣカードチップ１５０が非活性状態であるときに第１次ＩＣカード初期化処理あるいは第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図１２は、ＩＣカードチップ１５０が活性状態であるときに第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図１１と図１２において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００８２】図１１において１１０２は、図３に示したコールドリセットの信号波形を表す。図１２において１２０２は、図４に示したウォームリセットの信号波形を表す。図１１と図１２において、第１設定コマンド処理１１０４ａと１２０４ａ、第２設定コマンド処理１１０４ｂと１２０４ｂ、第Ｎ設定コマンド処理１１０４ｃと１２０４ｃは、それぞれ図５に示したＩＣカードコマンド処理の信号波形を表す。ＩＣカードチップ１５０の環境設定の信号波形１１０４と１２０４は、Ｎ個の設定コマンド処理の信号波形が連なって構成される。

【００８３】図１１と図１２において、１１０６と１２０６は、それぞれ図６に示した非活性化の信号波形を表す。図１１と図１２において、縦方向の破線１１０１、１１０３、１１０５、１１０７、１２０１、１２０３、１２０５、及び１２０７は、それぞれ特定の時刻を表す。１１０１はコールドリセット前の時刻、１２０１はウォームリセット前の時刻、１１０３はコールドリセッ

ト後から環境設定前の間にある時刻、１２０３はウォームリセット後から環境設定前の間にある時刻、１１０５と１２０５は環境設定後から非活性化前の間にある時刻、１１０７と１２０７は非活性化後の時刻である。

【００８４】図１１を参照して、第１次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＡが０のときは、信号波形に変化はない。Ａ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ａ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ａ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００８５】図１１を参照して、ＩＣカード制御パラメータＡが０または３のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００８６】図１２を参照して、ＩＣカード制御パラメータＡが１または２のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１２０１から時刻１２０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１２０１から時刻１２０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１２０１から時刻１２０７までの範囲の信号波形となる。Ｂ＝２かつＣ＝２のときは、時刻１２０３から時刻１２０５までの範囲の信号波形となる。Ｂ＝２かつＣ＝３のときは、時刻１２０３から時刻１２０７までの範囲の信号波形となる。Ｂ＝３のときは、時刻１２０５から時刻１２０７までの範囲の信号波形となる。

【００８７】図１３は、図７のステップ７１２において、ＣＰＵ１２１が、ホスト機器２２０が要求したセキュリティ処理をＩＣカードチップ１５０によって実行するときの手順を示すフローチャートである。セキュリティ処理を開始する（１３０１）と、まずＩＣカードチップ１５０が非活性状態かをチェックする（１３０２）。非活性状態ならば、ＩＣカードチップ１５０をコールドリセットし（１３０３）、ステップ１３０６に移る。活性状態ならば、ステップ１３０４に移る。ステップ１３０４では、ＩＣカードチップ１５０にＩＣカードコマンドを発行する前にＩＣカードチップ１５０を再リセットする必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０をウォームリセットし（１３０５）、ステップ１３０６に移る。必要がないならば、ステップ１３０６に移る。ステップ１３０６では、ＩＣカードチップ１５０の環境設定をおこなう必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０の環境設定をおこない（１３０７）、ステップ１３０８に移る。必要がないならば、ステップ１３０８に移る。ステップ１３０８では、ＩＣカードチップ１５０のＣＬＫ２端子に供給するクロック信号の周波数Ｆ２を設定する。そして、ＣＰＵ１２１はＩＣカードチップ１５０にセキュリティコマンドを発行し、ＩＣカードチップ１５０はそれを処理する（１３０９）。セキュリティコマンドの処理時間は、クロック周波数Ｆ２に依存する。

【００８８】次に、ＩＣカードチップ１５０が出力するＩＣカードレスポンスにより、その処理が成功したかどうかを判定する（１３１０）。成功ならば、ステップ１３１１に移る。失敗ならば、ステップ１３１２に移る。ステップ１３１１では、ＩＣカードチップ１５０に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ１３０４に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ１３１４に移る。ステップ１３１２では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない（１３１３）、ステップ１３０４に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをＣＰＵ１２１が再度準備することである。リトライできないならステップ１３１４に移る。これは、ホスト機器２２０が要求したセキュリティ処理が失敗したことを意味する。ステップ１３１４では、ＩＣカード制御パラメータＤをチェックする。Ｄ＝１ならば、ＩＣカードチップ１５０を非活性化して（１３１５）、セキュリティ処理を終了する（１３１６）。Ｄ＝１でないならば、ＩＣカードチップ１５０を活性状態に保ったままセキュリティ処理を終了する（１３１６）。

【００８９】図１３のフローチャートにおいては、クロック周波数Ｆ２を、ステップ１３０９で発行するセキュリティコマンドの種類によって変えることができるように、ステップ１３０８をステップ１３０９の直前に位置させたが、ステップ１３０８はそれ以外の位置にあってもよい。

【００９０】従来のＩＣカードへの攻撃法を有効にしている要因のひとつとして、ＩＣカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析においては、電気信号の測定においてＩＣカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、ＭＭＣ１１０内部でＩＣカードチップ１５０によりセキュリティ処理を実行するとき、

ホスト機器２２０はＩＣカードチップ１５０の駆動クロックを直接供給できない。ＣＰＵ１２１は、ＩＣカードチップ１５０へ供給するクロックの周波数Ｆ２を自由に設定することができる。これにより、ホスト機器２２０の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器２２０が高速なセキュリティ処理を要求するならば周波数Ｆ２を高く設定し、低い消費電力を要求するならば周波数Ｆ２を低く設定したり、クロックを適度に停止させればよい。

【００９１】また、ＣＰＵ１２１は、周波数Ｆ２だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ＩＣカードチップ１５０に対するタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理１回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ＩＣカードチップ１５０がＩＣカードコマンドを処理している時間の長さをホスト機器２２０が正確に計測できないためである。電力差分解析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分解析が困難になる理由は、ＩＣカードコマンドが発行された時刻、発行されたＩＣカードコマンドの内容、発行されたＩＣカードコマンドの順序（ＩＣカードコマンドを複数組み合わせてセキュリティ処理を実行する場合）の検出がホスト機器２２０にとって困難になるためである。故障利用解析の対策としては、ＩＣカードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、ＣＬＫ２制御回路１２７がＩＣカードチップ１５０に異常な駆動クロックを供給しないことが、ホスト機器２２０がＩＣカードチップ１５０に演算エラーを発生させるのを防止するからである。

【００９２】ＣＰＵ１２１は、ＩＣカードチップ１５０に供給するクロックの周波数Ｆ２、供給開始タイミング、及び供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＣＬＫ２設定情報２１１３として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００９３】図１４は、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程（図７のステップ７１０～７１２）において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスを簡単に表した図である。図１４において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００９４】図１４を参照して、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理要求ライトコマンドを送信する（１４０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理要求ライトコマンドのレスポンスを受信する（１４０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器２２０はＤＡＴ端子１４７にセキュリティ処理要求を送信する（１４０３）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１４０４）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、ホスト機器２２０から受信したセキュリティ処理要求をフラッシュメモリチップ１３０にライトするコマンドを発行する（１４０５）。セキュリティ処理要求をフラッシュメモリチップ１３０にライトすることにより、ＣＰＵ１２１がセキュリティ処理要求をＩＣカードコマンド形式で記述する処理（図７のステップ７１１）において、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。

【００９５】なお、フラッシュメモリチップ１３０にライトされたセキュリティ処理要求は、図２１においてセキュリティ処理バッファ領域２１１４に格納される。また、ライトコマンド発行１４０５は必須な操作ではない。ライト処理期間１４０６は、フラッシュメモリチップ１３０がセキュリティ処理要求のライト処理を実行している期間を表す。セキュリティ処理１４０７はＩＣカードチップ１５０によるセキュリティ処理の信号波形を

表す。この信号波形は図１３のフローチャートの遷移過程に依存する。セキュリティ処理１４０７は、ライト処理期間１４０６とオーバラップさせることができる。一般にフラッシュメモリチップ１３０のライト処理期間１４０６はミリ秒のオーダーであるため、セキュリティ処理１４０７とオーバラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。リード／ライト１４０８は、セキュリティ処理１４０７の実行中に、フラッシュメモリチップ１３０からセキュリティ処理要求をリードしたり、ＩＣカードチップ１５０が出力した計算結果をフラッシュメモリチップ１３０にライトするアクセスを示している。このアクセスにより、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト１４０８は必須ではない。セキュリティ処理１４０７が完了したら、ＭＭＣ１１０はＤＡＴ端子１４７をＨレベルにセットする（１４０９）。ＭＭＣ１１０は、これによりセキュリティ処理が完了したことをホスト機器２２０に示す。

【００９６】図１５は、図１４におけるセキュリティ処理１４０７の信号波形の一例を表した図である。図１５において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１５０１は図３に示したコールドリセットの信号波形を表し、１５０４は図４に示したウォームリセットの信号波形を表し、１５０２および１５０５は図１１（あるいは図１２）に示した環境設定の信号波形を表し、１５０３および１５０６および１５０７は図５に示したＩＣカードコマンド処理の信号波形を表し、１５０８は図６に示した非活性化の信号波形を表す。ＩＣカードチップ１５０の外部端子において図１５に示した信号波形が観測されるのは、図１３のフローチャートが１３０１、１３０２、１３０３、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０５、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０６、１３０８、１３０９、１３１０、１３１１、１３１４、１３１５、１３１６の順で遷移するときである。

【００９７】図１５を参照して、図１４のセキュリティ処理１４０７の実行中におけるＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセス（リード／ライト１４０８）を説明する。このアクセスには、図２１におけるセキュリティ処理バッファ領域２１１４を使用する。リード１５０９、１５１１、及び１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、及び１５０７においてＩＣカードチップ１５０に送信するＩＣカードコマンドを構築するために必要なデータを、フラッシュメモリチップ１３０からリードするアクセスである。ライト１５１０は、セキュリティコマンド処理１５０３においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にライトするアクセスである。ライト１５１３は、セキュリティコマンド処理１５０６及び１５０７においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にまとめてライトするアクセスである。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７以前のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。ライト１５１０、１５１３は、それぞれ、セキュリティコマンド処理１５０３、１５０７以後のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。これらのオーバラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。さらに、フラッシュメモリチップ１３０のライト単位が大きい場合は、ライト１５１３のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ１３０へのライト回数を削減し、フラッシュメモリチップ１３０の劣化を遅らせる効果がある。なお、ライト１５１０、１５１３でフラッシュメモリチップ１３０にライトする内容は、ＩＣカードチップ１５０が出力した計算結果そのものに限定されず、図７のステップ７１５でホスト機器２２０に返すセキュリティ処理結果またはその一部であってもよい。この場合、図７のステップ７１４またはその一部は、ステップ７１２の中で実行されることになる。

【００９８】図１６は、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程（図７のステップ７１３～７１５）において、ＭＭＣ１１０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスを簡単に表した図である。図１６において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、及びＤＡＴ端子１４７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００９９】図１６を参照して、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理結果リードコマンドを送信する（１６０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理結果リードコ

マンドのレスポンスを受信する（１６０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理結果ではない。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１６０３）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）から、ＩＣカードチップ１５０が出力した計算結果をリードする（１６０４）。ＣＰＵ１２１は、これをもとにセキュリティ処理結果を構築し、ＭＭＣ１１０がＤＡＴ端子１４７にセキュリティ処理結果を出力する（１６０５）。なお、図７のステップ７１４またはその一部が、ステップ７１２の中で実行されている場合、ステップ１６０４ではフラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）を利用しないでセキュリティ処理結果を構築する場合、ステップ１６０４は必要ない。

【０１００】ＭＭＣ１１０の製造者や管理者は、セキュリティシステムのユーザにＭＭＣ１１０を提供する前やそのユーザが所有するＭＭＣ１１０に問題が発生した時に、ＭＭＣ１１０に内蔵されたＩＣカードチップ１５０に様々な初期データを書きこんだり、ＩＣカードチップ１５０のテストをおこなったりする必要がある。ＭＭＣ１１０の製造者や管理者によるこれらの操作の利便性を高めるために、ＭＭＣ１１０は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるインタフェース機能を持つ。これにより、図３～図６で示したようなＩＣカードチップ１５０へのアクセス信号を、ＭＭＣ外部端子１４０から直接送受信できる。このようなＭＭＣ１１０の動作モードを、ＭＭＣ仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

【０１０１】インタフェース直通モードについて詳細に説明する。図１７は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるときの対応関係の一例を表した図である。この例では、ＲＳＴ端子１５２をＣＳ端子１４１に割り付け、ＧＮＤ２端子１５５をＧＮＤ１端子１４３、１４６に割り付け、ＶＣＣ２端子１５１をＶＣＣ１端子１４４に割り付け、ＣＬＫ２端子１５３をＣＬＫ１端子１４５に割り付け、Ｉ／Ｏ端子１５７をＤＡＴ端子１４７に割り付ける。このとき、ＣＳ端子１４１とＣＬＫ１端子１４５は入力端子、ＤＡＴ端子１４７は入出力端子として機能する。

【０１０２】ＭＭＣ１１０は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻すことができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図１を参照して、ＭＭＣＩ／Ｆ制御回路１２３は、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８と接続されており、ＭＭＣ１１０がホスト機器２２０から直通化コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けをおこなう。ＭＭＣ１１０がホスト機器２２０から復帰コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭＭＣ仕様に準拠した動作モードに戻る。

【０１０３】インタフェース直通モードでは、ホスト機器２２０がＩＣカードチップ１５０に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけにする必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

【０１０４】図１８は、ホスト機器２２０が、ＭＭＣ１１０の動作モードをＭＭＣ仕様に準拠した動作モードからインタフェース直通モードに移し、ＩＣカードチップ１５０に直接アクセスし、その後、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻すまでの処理手順を示すフローチャートである。ホスト機器２２０は処理を開始し（１８０１）、まずＭＭＣ１１０に直通化コマンドを発行する（１８０２）。ＭＭＣ１１０は、直通化コマンドで送信されたパスワードが正しいかチェックする（１８０３）。正しければステップ１８０４に移り、間違っていれば処理は終了する（１８１０）。ステップ１８０４では、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする。そして、図１７で示した端子割り付けをおこないインタフェースを直通化する（１８０５）。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする（１８０６）。ホスト機器２２０がＩＣカードチップ１５０への直接アクセスを終了し、ＭＭＣ１１０の動作モードを再びＭＭＣ仕様に準拠した動作モードに戻すときは、ＭＭＣ１１０に復帰コマンドを発行する（１８０７）。すると、ＣＰＵ１２１は図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭＭＣ仕様に準拠した動作モードに戻る（１８０８）。そして、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（１８０９）。以上で、処理は終了する（１８１０）。

【０１０５】図１９は、図１８のステップ１８０１～１８０６の過程において、ＭＭＣ１１０およびＩＣカード

チップ１５０の外部端子の信号波形を簡単に表した図である。図１９において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１９０５は、図３のコールドリセットの信号波形を示す。モード移行時刻１９０６は、動作モードがインタフェース直通モードに移る時刻を表す。

【０１０６】図１９を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをＭＭＣ仕様に準拠した動作モードからインタフェース直通モードに移しＩＣカードチップ１５０に直接アクセスする過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に直通化コマンドを入力すると（１９０１）、ＣＭＤ端子１４２から直通化コマンドのレスポンスが出力される（１９０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。次に、ホスト機器２２０はＤＡＴ端子１４７にパスワードを入力する（１９０３）。パスワード入力後、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力し（１９０４）、ビジー状態であることをホスト機器２２０に示す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする（１９０５）。そして、モード移行時刻１９０６において、動作モードをインタフェース直通モードに移す。このときに、ＤＡＴ端子１４７はＬレベルからハイインピーダンス状態になる。これにより、ホスト機器２２０はビジー状態の解除を知ることができる。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする。例えば、ＣＬＫ１端子１４５にクロックを供給すると（１９０７）、ＣＬＫ２端子１５３にそのクロックが供給される（１９０８）。また、ＤＡＴ端子１４７にＩＣカードコマンドを送信すると（１９０９）、Ｉ／Ｏ端子１５７にそのＩＣカードコマンドが送信される（１９１０）。

【０１０７】図２０は、図１８のステップ１８０７～１８１０の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図２０において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。モード復帰時刻２００３は、動作モードがインタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻る時刻を表す。２００４は、図６の非活性化の信号波形を示す。

【０１０８】図２０を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをインタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻す過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に復帰コマンドを入力すると（２００１）、ＣＭＤ端子１４２から復帰コマンドのレスポンスが出力される（２００２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。そして、モード復帰時刻２００３において、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力してビジー状態であることをホスト機器２２０に示し、それと同時に動作モードをＭＭＣ仕様に準拠した動作モードに戻す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（２００４）。そして、ＭＭＣ１１０は、ＤＡＴ端子１４７をハイインピーダンス状態にし（２００５）、復帰コマンドの処理が完了したことをホスト機器２２０に示す。これ以後、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスできない。ホスト機器２２０が、ＣＬＫ１端子１４５にクロックを供給しながらＣＭＤ端子１４２に何らかのメモリカードコマンドを送信した場合、ＩＣカードチップ１５０にそのクロック信号（２００６）は伝わらない。２００１及び２００２においてホスト機器２２０がＣＬＫ１端子１４５に供給するクロック信号は、ＩＣカードチップ１５０のＣＬＫ２端子１５３にも伝わるが、ＤＡＴ端子１４７がハイインピーダンス状態であるため、ＩＣカードチップ１５０がＩＣカードコマンドを誤って認識することはない。

【０１０９】図２１において、セキュリティ処理ステータス領域２１１６には、ＩＣカードチップ１５０によるセキュリティ処理の進捗状況を示す情報を格納する。ＣＰＵ１２１は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でＭＭＣ１１０への電源供給が停止した場合、電源供給再開時にＣＰＵ１２１がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

【０１１０】本発明におけるＭＭＣ１１０は、コントローラチップ１２０、フラッシュメモリチップ１３０及びＩＣカードチップ１５０の三つのうち二つ以上のチップで同時に処理を行うことで、処理の高速化及び処理時間の短縮を図ることができる。以下、本発明を適用したＭＭＣ１１０で行える並列処理の動作について説明する。

図２７は、並列に処理できるデータリード処理の手順を示したフローチャートである。ホスト機器２２０とＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態２７０１、待機状態２７１９となっている。ホスト機器２２０がＭＭＣ

１１０のＣＭＤ端子１４２に第一コマンドを送信すると（２７０２）、ＭＭＣ１１０は、第一コマンドを受信し（２７０９）、第一レスポンスを返す（２７１０）。ここで、レスポンスとは、コマンドを受け取ったＭＭＣ１１０がホスト機器２２０に返すデータのことである。単にコマンドを受信したら返すデータであるので、レスポンスを返すことがコマンドの実行が終了したことを意味しない。

【０１１１】ＭＭＣ１１０のコントローラチップ１２０は、第一コマンドを解釈し、フラッシュメモリチップ１３０又はＩＣカードチップ１５０に制御命令を発し第一処理に入る（２７１５）。ホスト機器２２０は、第一レスポンスを受け取ると第二コマンドを送信する（２７０４）。ＭＭＣ１１０のコントローラチップ１２０は、第一処理を実行しながら、ホスト機器２２０より第二コマンドを受信し、（２７０５）、第二レスポンスを返す（２７１２）。コントローラチップ１２０は、第二コマンドを解釈し、第二処理を実行する（２７１３）。

【０１１２】第二コマンドは、あらかじめ第一コマンドと同時に処理できるコマンドをホスト機器２２０で判定し設定する。また、同時に処理できるコマンドの判定は、コントローラチップ１２０でおこなってもよい。以下、同時に実行できるコマンドのことを並列実行可能なコマンドと呼ぶ。並列実行可能なコマンドとしては、例えば、フラッシュメモリチップ１３０にアクセスするコマンドとＩＣカードチップ１５０にアクセスするコマンド等の異なったチップにアクセスするコマンドである。例えば、フラッシュメモリチップ１３０から音楽データを読み出すコマンドが第一コマンドに相当し、暗号化されたデータを復号化する処理を実行するコマンドが第二コマンドに相当する。

【０１１３】第一処理が終了すると、コントローラチップ１２０は、ホスト機器２２０に第一データを送信する（２７１６）。その後、第二データを送信する（２７１４）。第一データ及び第二データの区別は、ＭＭＣ１１０のコントローラチップ１２０とホスト機器２２０のホストインターフェース２２３でデータに識別情報を付加して管理判断する。以下、識別情報を付加したデータをデータと呼ぶ。

【０１１４】また、第一処理の転送が終了して、第二処理をしている間にホスト機器２２０が並列実行可能なコマンドを第三コマンドとして発行した場合は、コントローラチップ１２０は、第二処理の実行とあわせて第三コマンドのコマンドを解釈し、第三処理を実行する（２７１７）。もし第一コマンドが大容量のデータ（ストリームデータ等）を要求するコマンドであるならば、第三処理を実行し（２７１７）、第二データの送信の終了を待ち、第三データを送信する（２７１８）。その後ホスト機器２２０からコマンドがなければ、ＭＭＣ１１０は待機状態になる（２７１９）。ホスト機器２２０はＭＭＣ１１０から必要なデータを受け取ると、待機状態になる（２７０１）。

【０１１５】図２８は、リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。ホスト機器２２０は、ＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（２７０２）。コントローラチップ１２０は、第一コマンドを解釈し、フラッシュメモリチップ１３０に制御命令を出す。第一処理中（２７１５）に、ホスト機器２２０は、並列実行可能なコマンドを第二コマンドとしてＭＭＣ１１０のＣＭＤ端子１４２に送信する（２７０４）。コントローラチップ１２０は、第二コマンドを解釈し、ＩＣカードチップ１５０に制御命令を出し、第二処理を実行する（２７１３）。ＭＭＣ１１０は、第一データ２８０３、第二データ２８０４のように順にデータを転送する。第二処理（２７１３）中にホスト機器２２０が第三コマンドとしてフラッシュメモリチップ１３０にアクセスするコマンドを発行した場合（２８０１）、コントローラチップ１２０はフラッシュメモリチップに制御命令を出す。ＭＭＣ１１０は、第二データ２８０４の転送終了を待って、第三データ２８０５を転送する。また第三データ２８０５は、第一コマンドが大容量データ（ストリームデータ等）を送るコマンドでもよい。その場合は、第三コマンドの発行（２８０１）と第三レスポンス（２８０２）の信号はなくてもよい。以上の処理内容は、コントローラチップ１２０が制御命令を出す対象としてフラッシュメモリチップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆の場合でもよい。

【０１１６】図２９は、並列に処理できるデータライト処理の流れを示した図である。ホスト機器２２０とＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態２９０１及び待機状態２９１０となっている。ホスト機器２２０がＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（２９０２）。ＭＭＣ１１０は、第一コマンドを受信し（２９１１）、第一レスポンスを返し（２９１２）、同時に第一データを受信し（２９１３）、データ端子１４７からデータを転送できないようにする。これを以下ビジー状態と呼ぶ。ＭＭＣ１１０はホスト機器２２０からデータを受け取った後ビジー状態にしなくても良い。第一データを受信するステップ２９１３は、第一レスポンス（２９１２）と同時でなくても良い。

【０１１７】ホスト機器２２０は、第一レスポンスを受信し（２９０３）、並列実行可能なコマンドを第二コマンドとして、ＣＭＤ端子１４２に送信する（２９０４）。ＭＭＣ１１０は、ホスト機器２２０より第二コマンドを受信し（２９１４）、第一データを受信（２９１３）中であれば受信し、第二レスポンスを送信し（２９１５）、第二処理を開始する（２９２０）。データビジ

ー状態であれば、第二処理で行うアドレス設定まで行い、第二データの転送を待つ。第二処理はアドレス設定のみだけでなく実行可能な処理を続けてもよい。ホスト機器２２０は、第二レスポンスを受信し（２９０５）、ビジー状態の解除を待って、第二データを送信する（２９０７）。第一コマンドが大容量データ（ストリームデータ等）を転送する場合、ＭＭＣ１１０は、第二処理中（２９２０）に第三処理を開始し（２９２１）、第三データの転送（２９０８）を待つ。ＭＭＣ１１０は、ビジー状態が解除されたら、第三データを受信し（２９１８）、第三処理を続ける。その後ホスト機器２２０からコマンドがなければ、ＭＭＣ１１０は待機状態になる（２９１０）。ホスト機器２２０はＭＭＣ１１０に必要なデータを転送し終わると、待機状態になる（２９０１）。

【０１１８】図３０は、ライトコマンドを並列処理する時のコマンドとデータの流れ及び処理を時間軸にそって示した図である。ホスト機器２２０がフラッシュメモリチップ１３０にデータをライトする第一コマンドをＭＭＣ１１０のＣＭＤ端子１４２に送信し（２９０２）、第一レスポンスを待ち（２９０３）、第一データを送信する（３００３）。ＭＭＣ１１０は、第一コマンドを受けると第一レスポンスを送信し（２９０３）、フラッシュメモリチップ１３０に制御命令を出し（第一処理２９１６）、ビジー状態となる。ここでビジー状態にしなくてもよい。ホスト機器２２０は、第一データ３００３を送信しながら並列実行可能なコマンドとしてＩＣカードチップ１５０にデータを転送する第二コマンドを送信する（２９０４）。ホスト機器２２０は、第二レスポンスを受信し（２９０５）、ビジー状態の解除を待って第二データ３００４を送信する。コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令を出し、第二処理を開始して、第二データ３００４を待つ。ホスト機器２２０は、ビジー状態が解除されるとＩＣカードチップ１５０に送信する第二データ３００４を転送する。

【０１１９】ＭＭＣ１１０は、第二データを受信すると（２９１７）、ビジー状態になる。ＩＣカードチップ１５０が処理中（第二処理中２９２０）に、ホスト機器２２０がフラッシュメモリチップ１２０にアクセスする第三コマンドの発行すると（３００１）、ＭＭＣ１１０は、第三レスポンスを送信し（３００２）、コントローラチップ１２０はフラッシュメモリチップに制御命令を出し、第三処理を開始する（２９２１）。ホスト機器２２０は、ビジー状態の解除を待って第三データを送信する（３００５）。もしフラッシュメモリチップ１３０にアクセスする第一コマンドが大容量データ（ストリームデータ等）を転送する場合は、ICカードチップ１５０の処理中（第二処理２９２０）のビジー状態の解除を待って、ホスト機器２２０は、フラッシュメモリチップ１３０に第三データ３００５を送信する。ＭＭＣ１１０は、第三データ３００５を受信し、フラッシュメモリチップ１３０に制御命令を出し第三処理を行う。

【０１２０】以上の処理内容は、コントローラチップ１２０が制御命令を出す対象としてフラッシュメモリチップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆の場合でもよい。

【０１２１】図３１は、並列に処理できるデータを転送しないコマンドの処理を示した図である。ホスト機器２２０及びＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３１０１、待機状態３１１０となっている。ホスト機器２２０はＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（３１０２）。ＭＭＣ１１０は、第一コマンドを受信し（３１１１）、第一レスポンスをホスト機器２２０に送信し（３１１２）、第一処理を開始する（３１１６）。ホスト機器２２０はＭＭＣ１１０からの第一レスポンスを受信すると（３１０３）、並列実行可能なコマンドを第二コマンドとして送信する（３１０４）。ＭＭＣ１１０は、第二コマンドを受信すると（３１１３）、ホスト機器２２０に対し第二レスポンスを送信し（３１１４）、第二処理を実行する（３１１５）。その後処理が終わると、ホスト機器２２０は待ち状態３１０１、ＭＭＣ１１０は待ち状態３１１０の状態となる。

【０１２２】図３２は、並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。ホスト機器２２０は、ＭＭＣ１１０のＣＭＤ端子１４２にデータ転送を行わないフラッシュメモリチップ１３０にアクセスする第一コマンドを送信する（３１０２）。ＭＭＣ１１０は、第一コマンドを受信し（３１１１）、コントローラチップ１２０は、フラッシュメモリチップ１３０に制御命令を出し、第一処理を開始する（３１１４）。ホスト機器２２０は、第一レスポンスを受信し（３１０３）、ＭＭＣ１０のＣＭＤ端子１４２にデータ転送を行わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３１０４）。ＭＭＣ１１０は、第二コマンドを受信し（３１１３）、コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令を出し第二処理を行う（３１１５）。ホスト機器２２０は、コントローラチップ１２０の内部処理のみで実行できるコマンドを第三コマンドとしてＭＭＣ１１０のＣＭＤ端子１４２に送信する（３２０１）。ＭＭＣ１１０は第三コマンドを受信し、第三処理を実行する（３２０３）。このとき、第一処理及び第二処理は実行中でもよい。

【０１２３】以上の処理の中で、第一コマンド及び第二コマンドは、フラッシュメモリチップ１３０にアクセスする処理、ＩＣカードチップ１５０にアクセスする処理、及びコントローラチップ１２０の内部処理の三処理のうちのどの二処理でもよい。また、連続コマンドが、

コントローラチップ１２０の内部処理のみで実行できるコマンドで、同様の処理を行うコマンドは、後で発行したコマンドだけを有効にしても良い。

【０１２４】図３３は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器２２０及びＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３３０１、待機状態３３１０となっている。ホスト機器２２０がＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（３３０２）。ＭＭＣ１１０は第一コマンドを受信し（３３１１）、第一レスポンスをホスト機器２２０に送信し（３３１２）、第一処理を開始する（３３１６）。ホスト機器２２０は、第一レスポンスを受信して（３３０３）、並列実行可能なコマンドを第二コマンドとして送信する（３３０４）。ＭＭＣ１１０は、第二コマンドを受信し（３３１３）、第二レスポンスを返す（３３１４）。その間にＤＡＴ端子１４７から、第一データを送信し（３３１７）、第二処理を開始する（３３１５）。ホスト機器２２０は、第一データを受信し（３３０６）、第二レスポンスを受信する（３３０５）。ホスト機器２２０は、並列処理可能なコマンドとして第三コマンドを送信する（３３０７）。ＭＭＣ１１０は、第三コマンドを受信し（３３１８）、第三レスポンスを返す（３３１９）。ホスト機器２２０は、第三レスポンス受信する（３３０８）。ＭＭＣ１１０は、第三処理３１２０を実行し、第二データを送信する（３３２１）。ホスト機器２２０は、第二データを受信する（３３０９）。その後実行するコマンドがなければ、ホスト機器２２０は、待ち状態３３０１に、ＭＭＣ１１０は、待ち状態３３１０になる。

【０１２５】図３４は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器２２０がＭＭＣ１１０のコマンド端子１４２にフラッシュメモリチップ１２０にアクセスする第一コマンドを送信する（３３０２）。ＭＭＣ１１０は第一レスポンスを返し（３３０３）、コントローラチップ１２０は、制御命令をフラッシュメモリチップ１３０に出し第一処理を開始する（３３１７）。ホスト機器２２０は、並列実行可能なデータ転送を伴わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３３０４）。ＭＭＣ１１０は第二コマンドを受信して（３３１３）、第二レスポンスを返し（３３０５）、コントローラチップ１２０はＩＣカードチップ１５０に制御命令を出し、第二処理を開始する（３３１５）。ＭＭＣ１１０は、第一処理が終了すると（３３１６）、第一データ３４０３をホスト機器２２０に送信する。ホスト機器２２０は、第一データを受信し（３３０６）、並列処理可能なフラッシュメモリチップ１３０にアクセスする第三コマンドを送信する（３３０７）。ＭＭＣ１１０は、第三レスポンスを返し（３３０８）、コントローラチップ１２０は第三処理を実行し（３３２０）、第二データを送信する（３４０５）。

【０１２６】以上の処理は、フラッシュメモリトップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆でもよい。また、データ転送を伴わないコマンドは、コントローラチップ１２０の内部処理を行うコマンドでもよい。第一コマンドが大容量データデータ（ストリームデータなど）を転送するコマンドの場合は、第三コマンドは、発行されなくても良い。

【０１２７】図３５は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器２２０及びＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３５０１、待機状態３５１０となっている。ホスト機器２２０がＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（３５０２）。ＭＭＣ１１０は第一コマンドを受信し（３５１１）、第一レスポンスをホスト機器２２０に送信する（３５１２）。ホスト機器２２０は、第一レスポンスを受信して（３５０３）、並列実行可能なコマンドを第二コマンドとして送信し（３５０４）、第一データを送信する（３５０５）。ＭＭＣ１１０は、第二コマンドを受信し（３５１３）、第二レスポンスを返す（３５１４）。その間にＤＡＴ端子１４７から、第一データを受信し（３５１６）ビジー状態になる。ＭＭＣ１１０は、第一データを受信したら（３５１６）、第一処理を開始し（３５１７）、第二処理を開始する（３５１５）。ホスト機器２２０は、ビジー状態が解除されると第三コマンドを送信（３５０７）する。ＭＭＣ１１０は第三レスポンスを返す（３５１９）。ホスト機器１１０は第三レスポンスを受信すると（３５０８）、第二データを送信する（３５０９）。ＭＭＣ１１０は、第二データを受信し（３５２０）、ビジー状態になり第三処理（３５２１）を実行する。処理が終了すると、ホスト機器２２０は、待ち状態３５０１となり、ＭＭＣ１１０は処理が終了すると待ち状態３５１０となる。以上の処理で、ＭＭＣ１１０がデータ受信後ビジー状態にならなくても良い。

【０１２８】図３６は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器２２０がフラッシュメモリチップ１３０にアクセスする第一コマンドを転送する（３５０２）。ＭＭＣ１１０は第一レスポンスを返し（３５０３）、第一データ受信し（３５０５）、コントローラチップ１２０はフラッシュメモリチップ１３０に制御命令を出し、第一処理を開始し（３５１７）、ビジー状態となる。ホスト機器２２０は、並列実行可能なデータ転送を伴わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３５０４）。ＭＭＣ１１０は第二コマンドを受信して（３５１

３）、第二レスポンスを返す（３５０６）。コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令をだし第二処理を開始する（３５１５）。その後ホスト機器２２０はビジー状態が解除されるのを待って、フラッシュメモリチップ１３０にアクセスする第三コマンドを送信する（３５０７）。ＭＭＣ１１０は、第三コマンドを受信し（３５１８）、第三レスポンスを返し（３５０８）、第二データ３５０９を受信する（３５２０）。コントローラチップ１２０は、フラッシュメモリチップ１３０に制御命令を出し、第三処理を開始しビジー状態になる（３５２１）。

【０１２９】以上の処理で、フラッシュメモリチップ１３０がＩＣカードチップ１５０に、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆になっても良い。データ転送を伴わない処理は、コントローラチップ１２０の内部処理でもよい。また、ＭＭＣ１１０がデータ受信後ビジー状態にならなくても良い。第一コマンドが大容量データ（ストリームデータ等）を転送するコマンドである場合、第三コマンドの発行と第三レスポンスは必要としない。

【０１３０】以上の動作は、図２４及び図２５で示す、ＳＤカードホスト機器２４６０とSDカード２４１０、メモリスティックホスト機器２５６０とメモリスティック２５１０のような構成で、コントローラを通してのＳＤカード内のＩＣカードチップ１５０とフラッシュメモリチップ２４３０、メモリスティック内のＩＣカードチップ１５０とフラッシュメモリチップ２５３０の同時アクセスの場合においても同様である。

【０１３１】以上のように、ホストからのコマンドに応じて、フラッシュメモリチップ１３０、ＩＣカードチップ１５０及びコントローラチップ１２０で並列処理が可能であるので処理を高速化及び処理時間を短縮することができる。したがって、一つのＭＭＣ１１０を用いて、音楽データを再生しながら、銀行からお金を引き落とす際の認証処理を行うことができる。

【０１３２】本発明の実施形態によれば、メモリカード外部からＩＣチップの駆動クロックを直接供給しないため、ＩＣチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分解析、故障利用解析攻撃法に対するセキュリティが向上する。

【０１３３】本発明の実施形態によれば、メモリカード外部からＩＣチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ＩＣチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ＩＣチップの駆動クロックの周波数を低くしたり、ＩＣチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

【０１３４】本発明の実施形態によれば、ＩＣチップによるセキュリティ処理に必要なデータや、ＩＣチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

【０１３５】本発明の実施形態によれば、ＭＭＣの製造者や管理者が、ＭＭＣ内部のＩＣチップに直接アクセスすることができる。したがって、ＭＭＣ内部のＩＣチップの初期化やメンテナンスを、従来のＩＣカードと同様な方法で実現できる。

【０１３６】本発明の実施形態によれば、フラッシュメモリチップを備えたＭＭＣに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたＩＣカードチップ追加搭載することによって、セキュリティ評価機関によるＭＭＣの認証が不要となるため、ＭＭＣの開発期間又は製造期間が短縮する。

【０１３７】本発明の実施形態によれば、ホスト機器からのコマンドに応じて、フラッシュメモリチップ、ＩＣカードチップ及びコントローラチップ１２０で並列処理が可能であるので処理を高速化することができる。

【０１３８】

【発明の効果】本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。また、記憶装置の処理を高速にすることができる。

【図面の簡単な説明】

【図１】本発明を適用したＭＭＣ１１０の内部構成を示す図である。

【図２】本発明を適用したＭＭＣ１１０のホスト機器２２０の内部構成、およびホスト機器とＭＭＣ１１０との接続状態を示す図である。

【図３】ＩＣカードチップのコールドリセット時の信号波形を示す図である。

【図４】ＩＣカードチップのウォームリセット時の信号波形を示す図である。

【図５】ＩＣカードチップのＩＣカードコマンド処理時の信号波形を示す図である。

【図６】ＩＣカードチップの非活性化時の信号波形を示す図である。

【図７】ホスト機器によるＭＭＣへのアクセスを示したフローチャートである。

【図８】ＩＣカード制御パラメータとそれに対応するＩＣカードへの処理内容を示す表である。

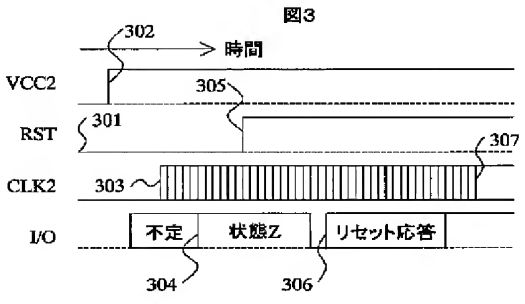
【図９】ＩＣカードチップに対する第１次ＩＣカード初期化の詳細なフローチャートである。

【図１０】ＩＣカードチップに対する第２次ＩＣカード初期化の詳細なフローチャートである。

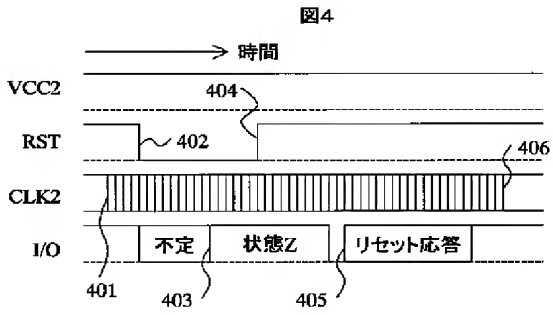
【図１１】非活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。

【図１２】活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。
【図１３】ＩＣカードチップによるセキュリティ処理の詳細なフローチャートである。
【図１４】セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
【図１５】ＩＣカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。
【図１６】セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
【図１７】インタフェース直通モードにおけるＭＭＣ外部端子とＩＣカードチップ外部端子の対応関係を示す図である。
【図１８】インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。
【図１９】インタフェース直通モードへ移行する処理時の信号波形を示す図である。
【図２０】インタフェース直通モードから復帰する処理時の信号波形を示す図である。
【図２１】フラッシュメモリチップの内部構成を示す図である。
【図２２】本発明を適用したＭＭＣの内部構成を簡単に示す図である。
【図２３】本発明を適用したＭＭＣをコンテンツ配信に応用した例を示す図である。
【図２４】本発明を適用したＳＤカードの内部構成を簡単に示す図である。
【図２５】本発明を適用したメモリースティックの内部構成を簡単に示す図である。
【図２６】本発明のＩＣカードチップの内部構成を示す図である。
＊【図２７】並列に処理できるデータリード処理の流れを示した図である。
【図２８】リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。
【図２９】並列に処理できるデータライト処理の流れを示した図である。
【図３０】ライトコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。
【図３１】並列に処理できるデータを転送しないコマンドの処理を示した図である。
【図３２】並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。
【図３３】並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。
【図３４】並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。
【図３５】並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。
【図３６】並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。
【符号の説明】
１１０…ＭＭＣ、１２０…コントローラチップ、１４０…ＭＭＣ外部端子、１５０…ＩＣカードチップ、１５１…ＶＣＣ２端子、１５２…ＲＳＴ端子、１５３…ＣＬＫ２端子、１５５…ＧＮＤ２端子、１５６…ＶＰＰ端子、１５７…Ｉ／Ｏ端子、２２０…ホスト機器、１４０５…ライトコマンド発行、１９０６…モード移行時刻、２００３…モード復帰時刻。

【図３】

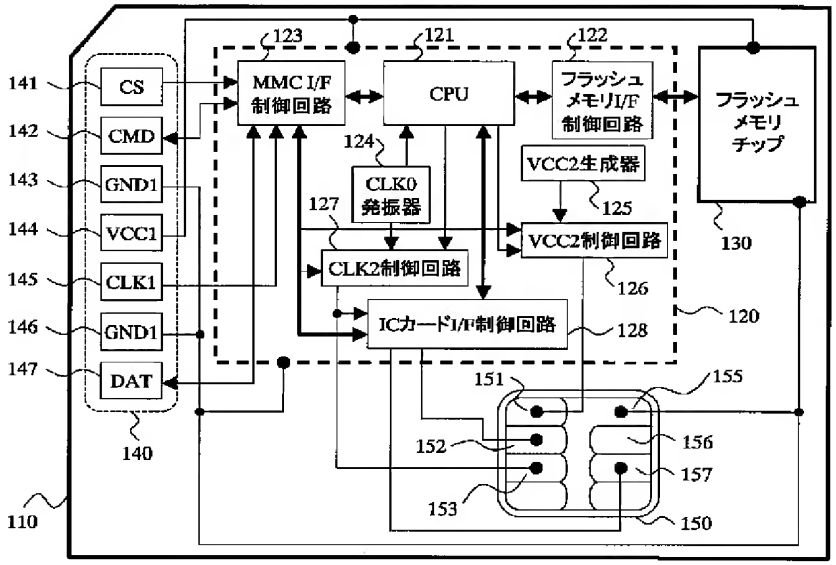


【図４】



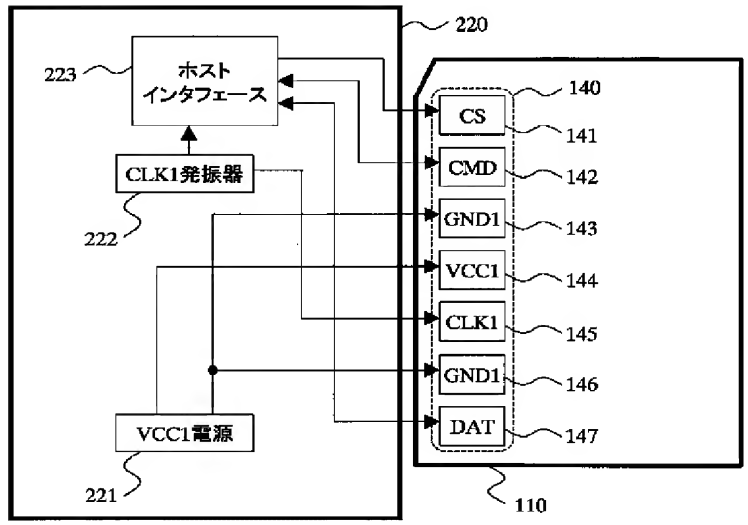
【図１】

図1



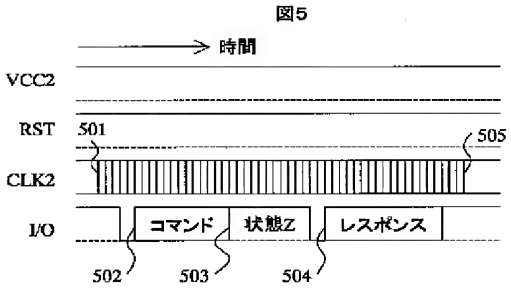
【図２】

図2



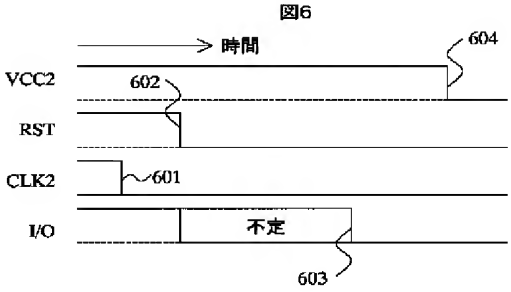
【図５】

図5



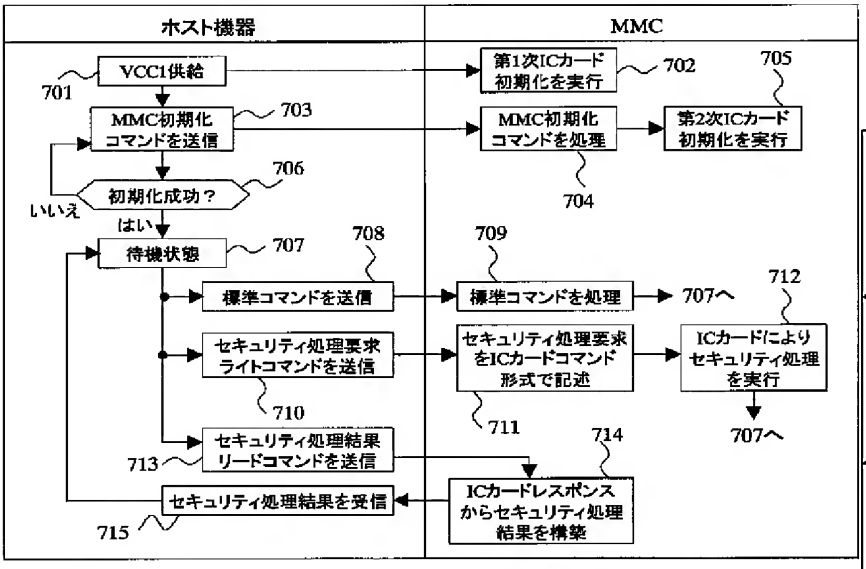
【図６】

図6



【図７】

図7



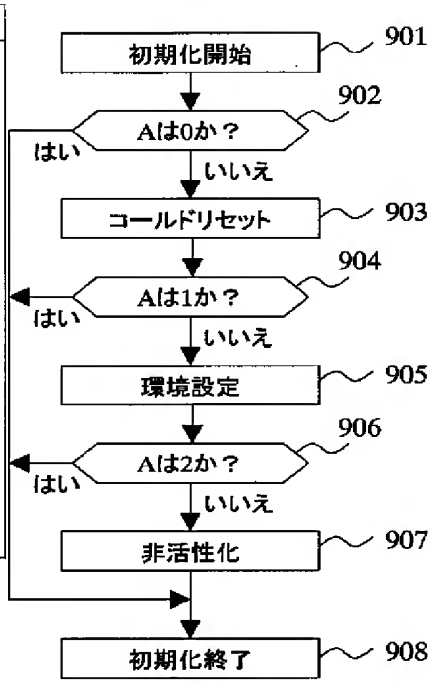
【図８】

図8

ICカード制御パラメータ		ICカードに対する処理
A=0		MMCのパワーオン時に，何もしない
A=1		MMCのパワーオン時に，リセット
A=2		MMCのパワーオン時に，リセットと環境設定
A=3		MMCのパワーオン時に，リセットと環境設定し，非活性化
B=0		MMCの初期化時に，何もしない
B=1	C=1	MMCの初期化時に，リセット
	C=2	MMCの初期化時に，リセットと環境設定
	C=3	MMCの初期化時に，リセットと環境設定し，非活性化
B=2	C=2	MMCの初期化時に，環境設定
	C=3	MMCの初期化時に，環境設定し，非活性化
B=3		MMCの初期化時に，活性状態ならば，非活性化
D=0		セキュリティ処理後に，非活性化しない
D=1		セキュリティ処理後に，非活性化する

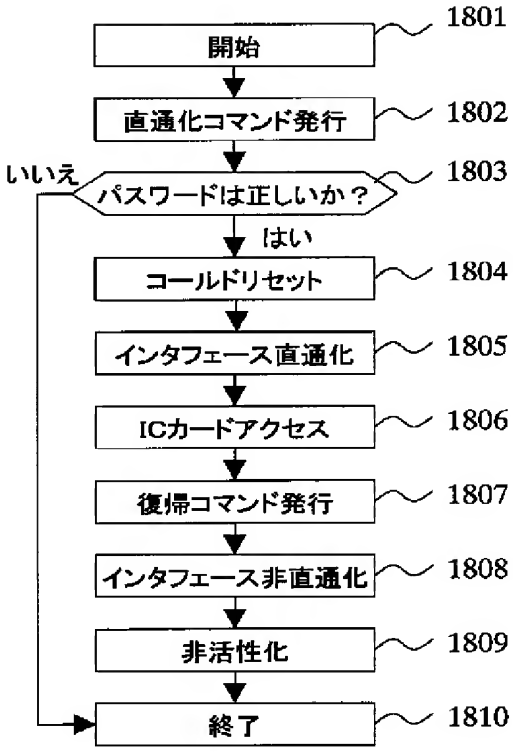
【図９】

図9



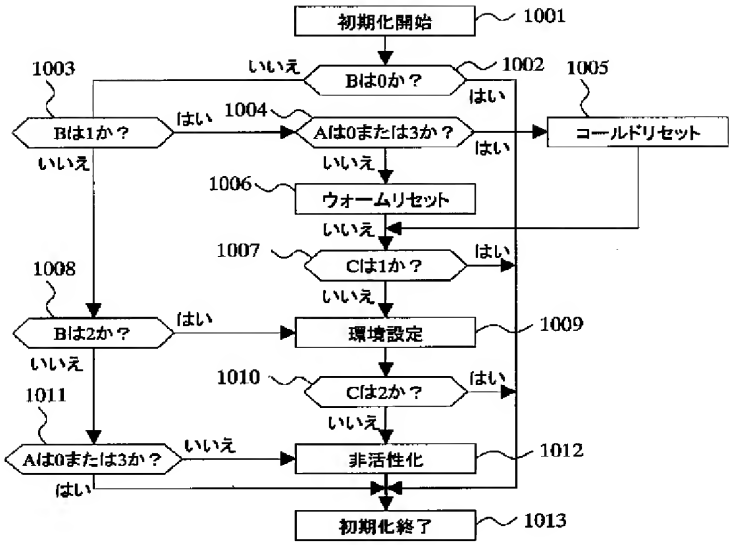
【図１８】

図18



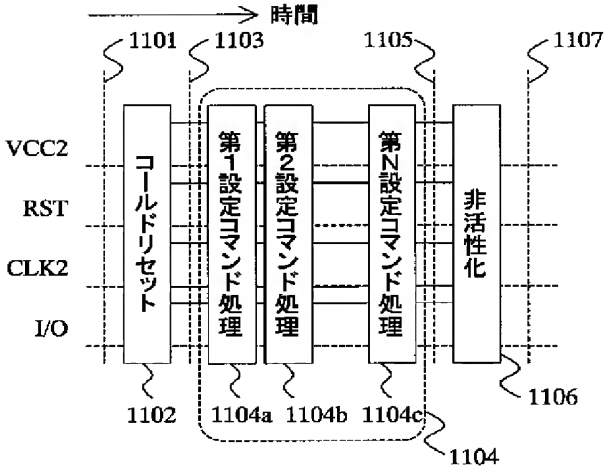
【図１０】

図10



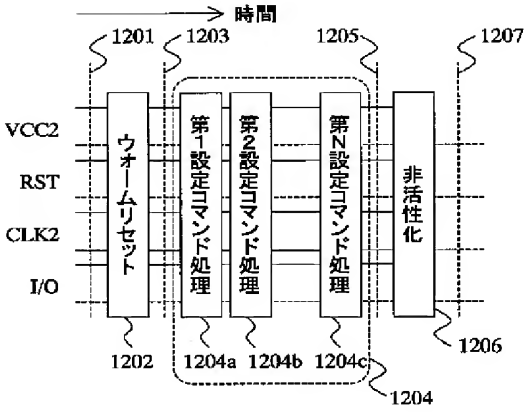
【図１１】

図11



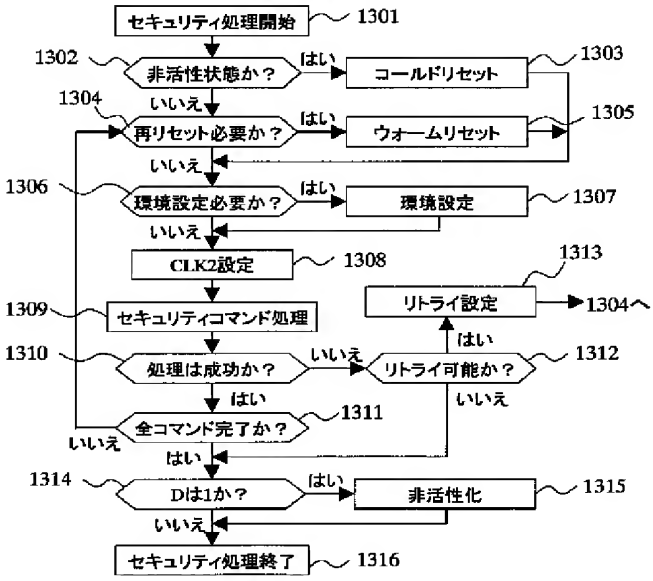
【図１２】

図12



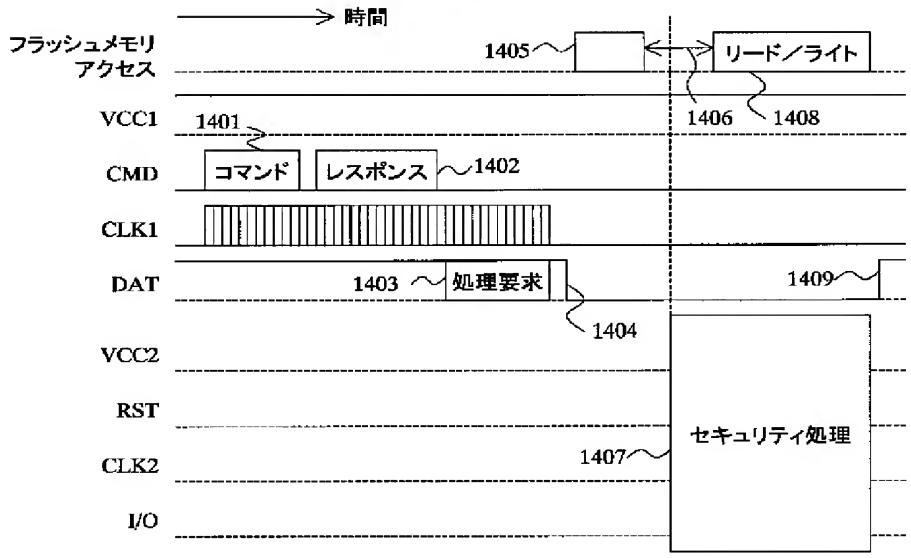
【図１３】

図13



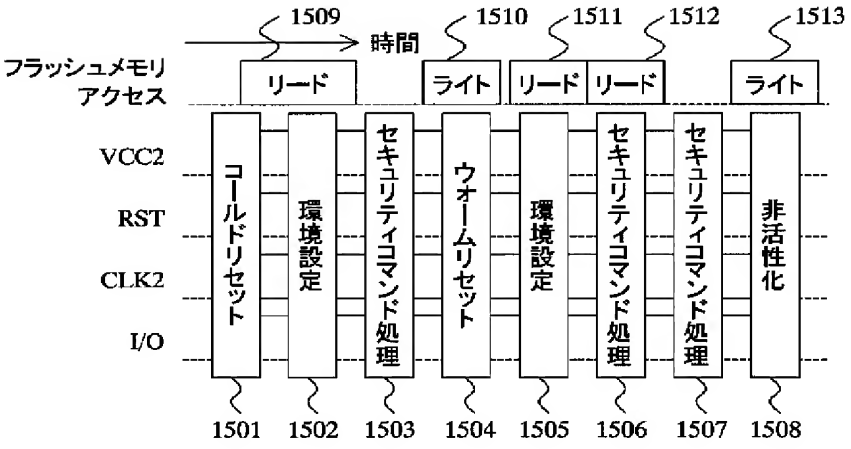
【図１４】

図14



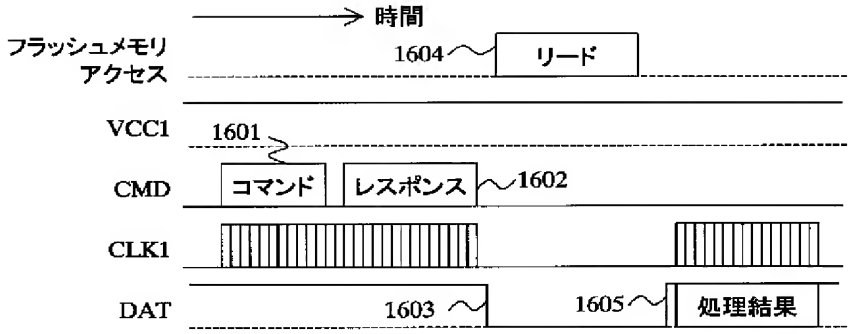
【図１５】

図15



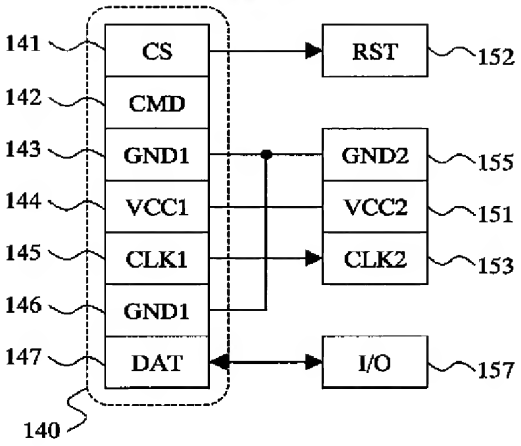
【図１６】

図16



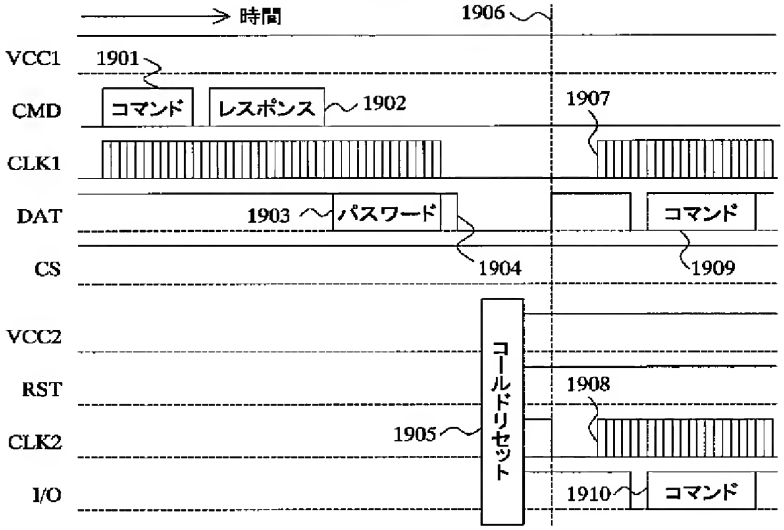
【図１７】

図17



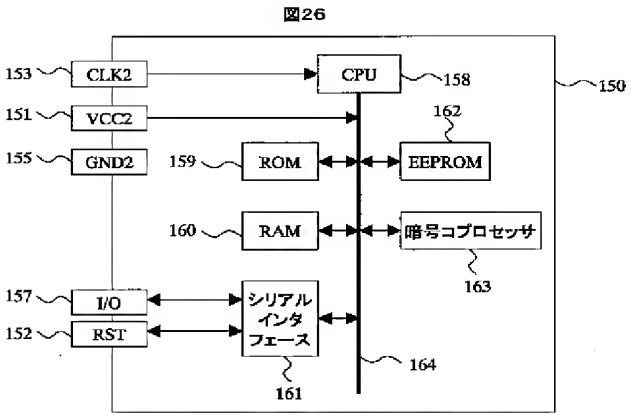
【図１９】

図19



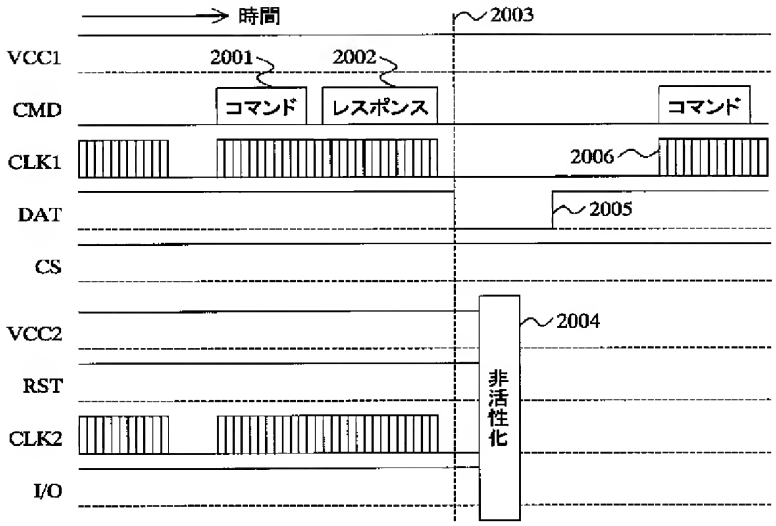
【図２６】

図26



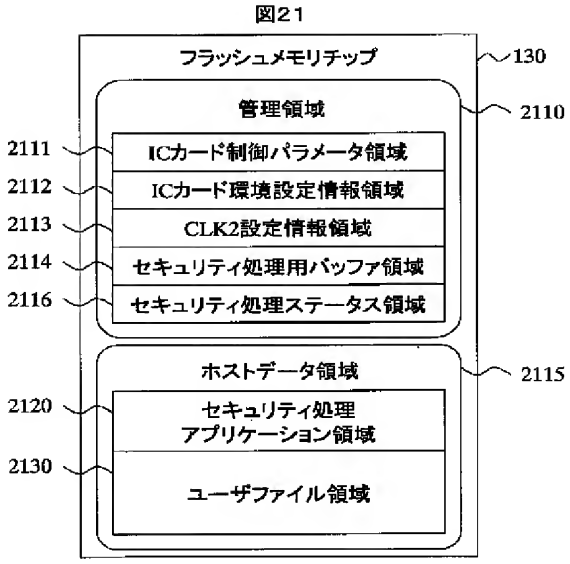
【図２０】

図20



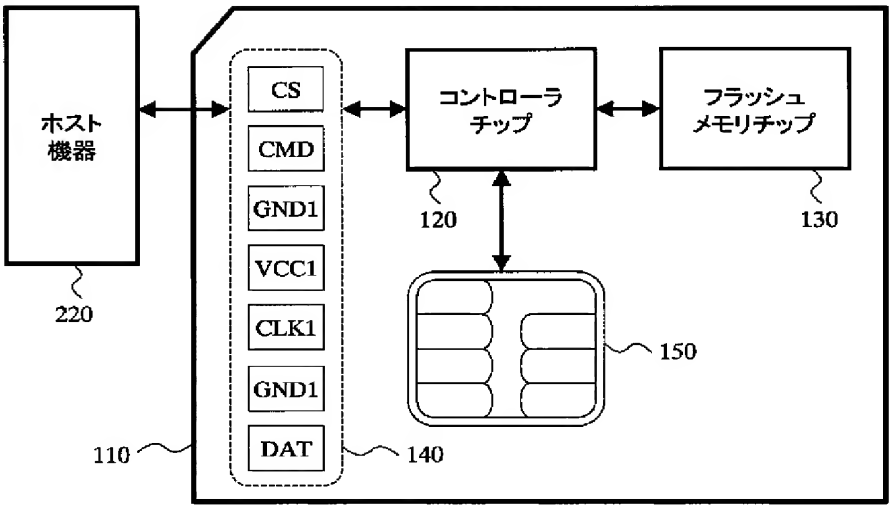
【図２１】

図21



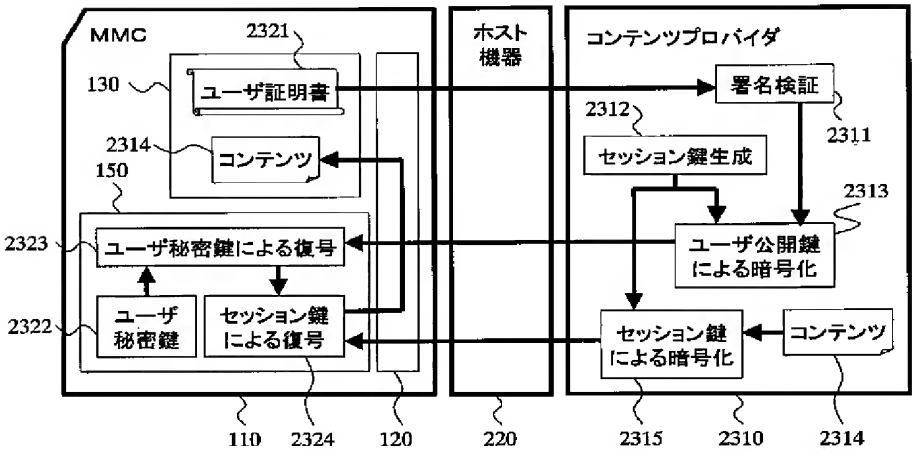
【図２２】

図22



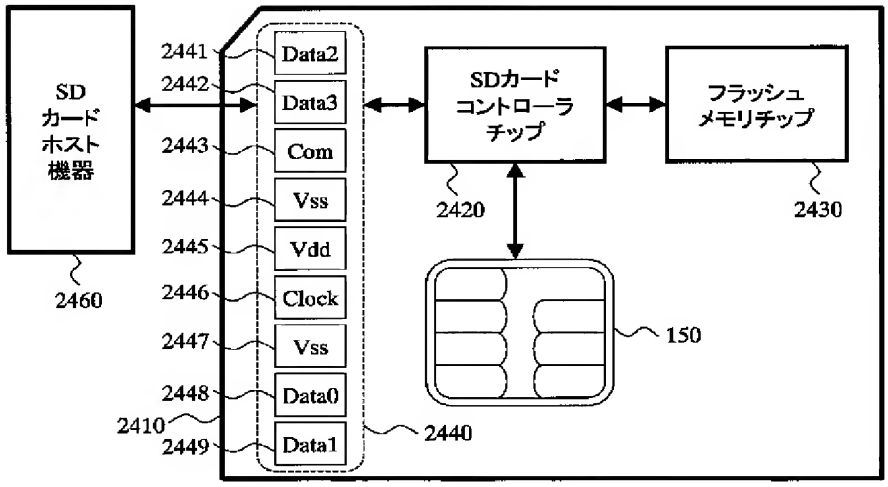
【図２３】

図23



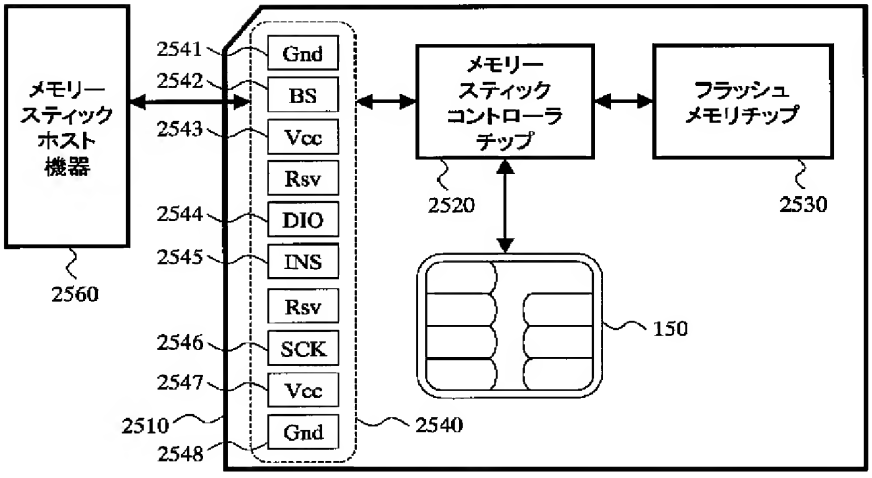
【図２４】

図24



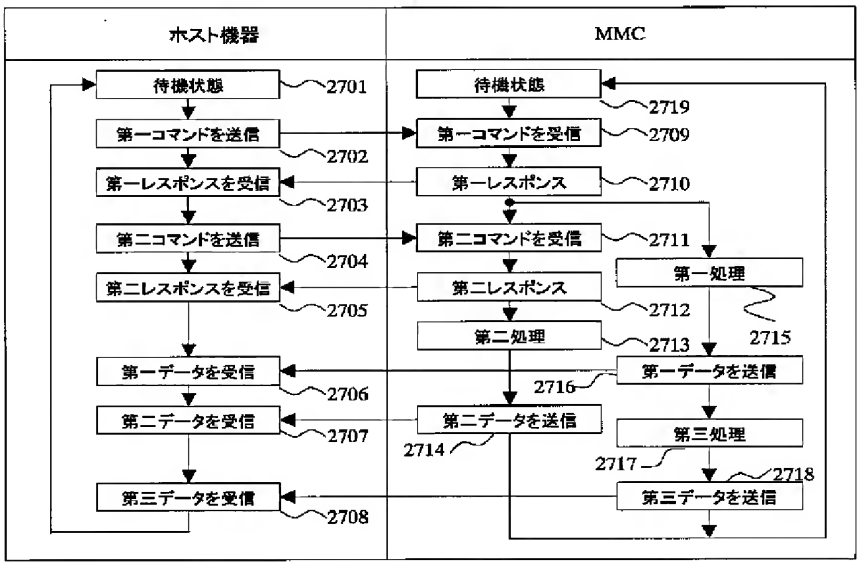
【図２５】

図25



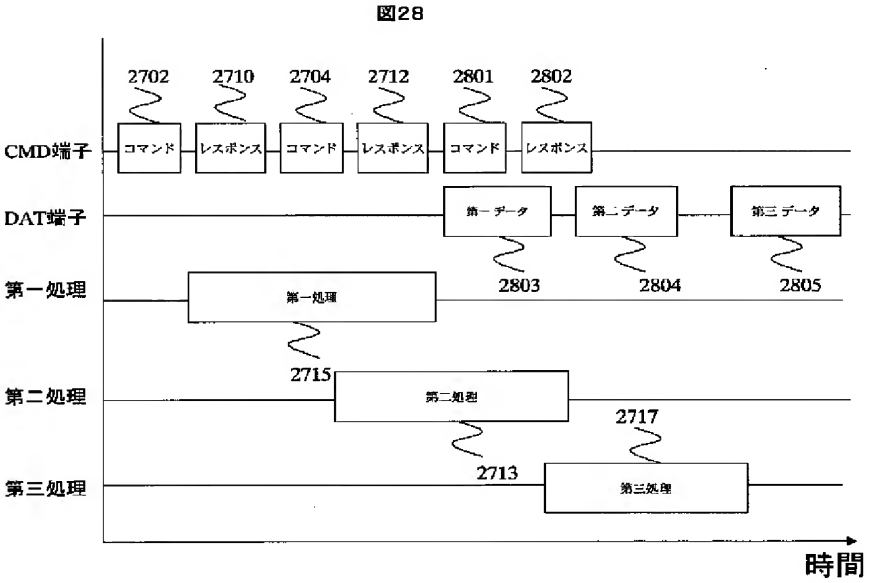
【図２７】

図27



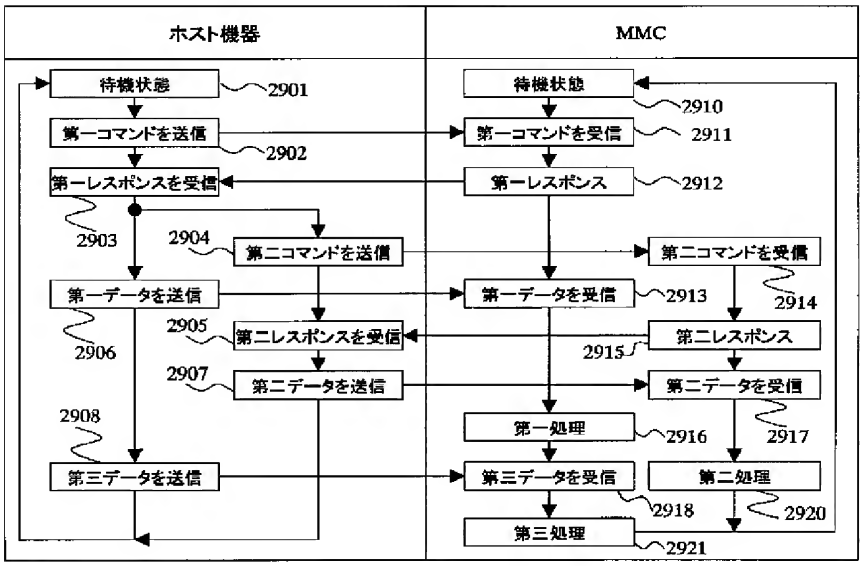
【図２８】

図28



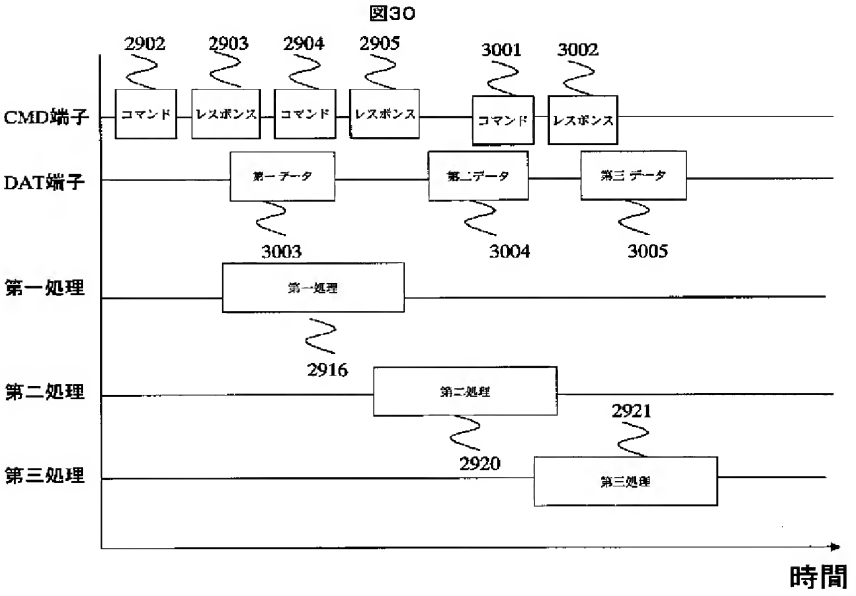
【図２９】

図29



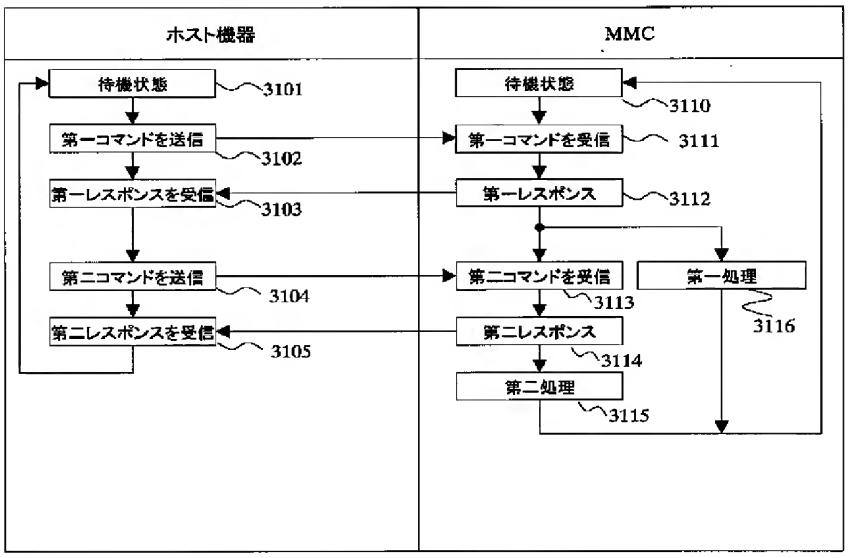
【図３０】

図30



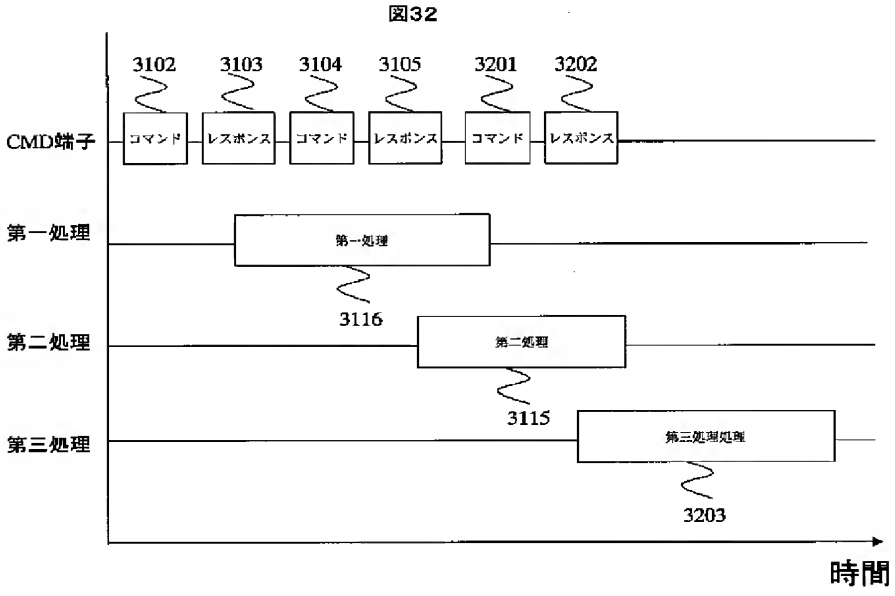
【図３１】

図31



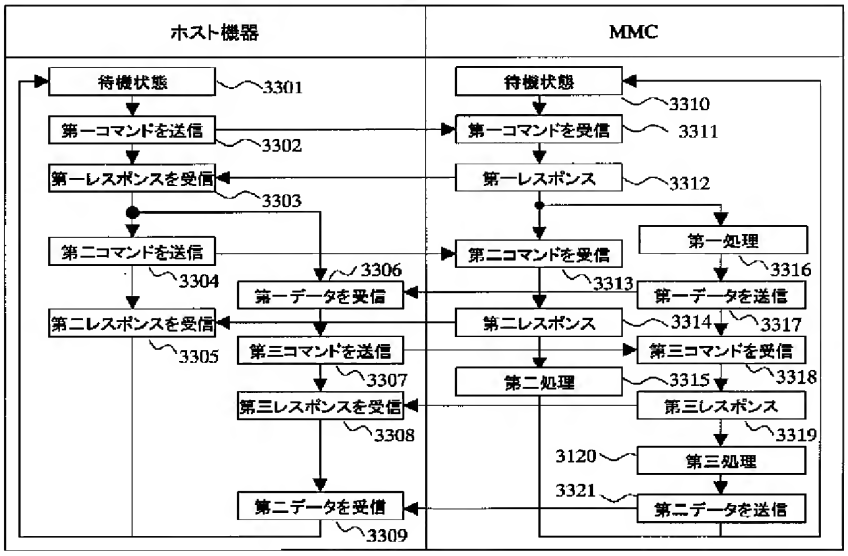
【図３２】

図32



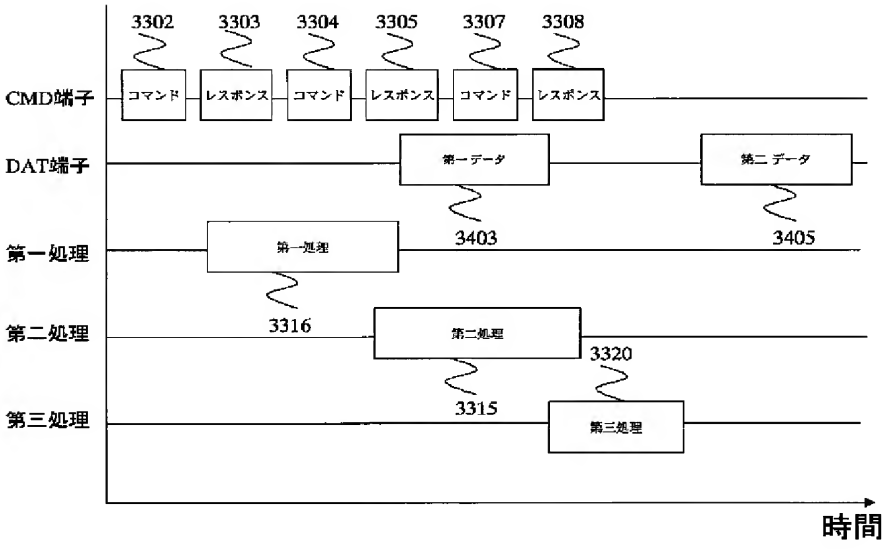
【図３３】

図33



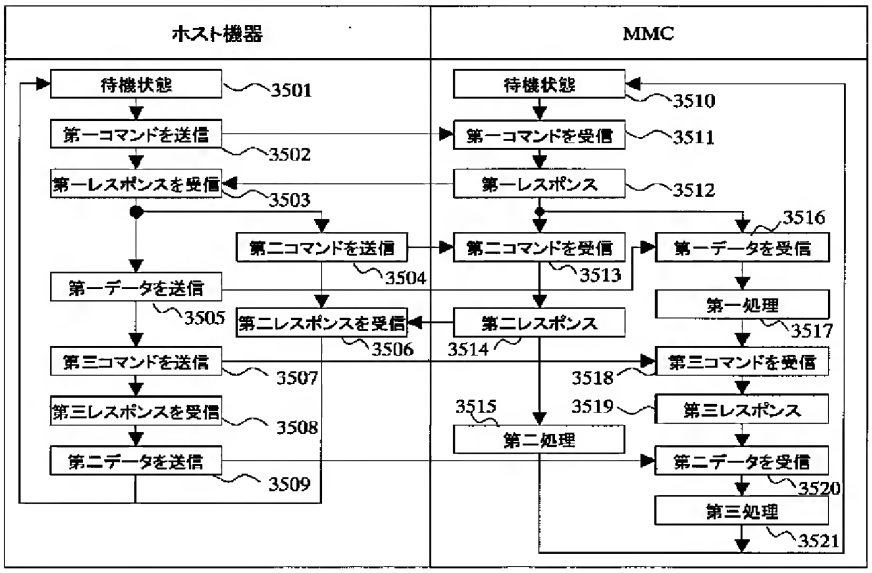
【図３４】

図34



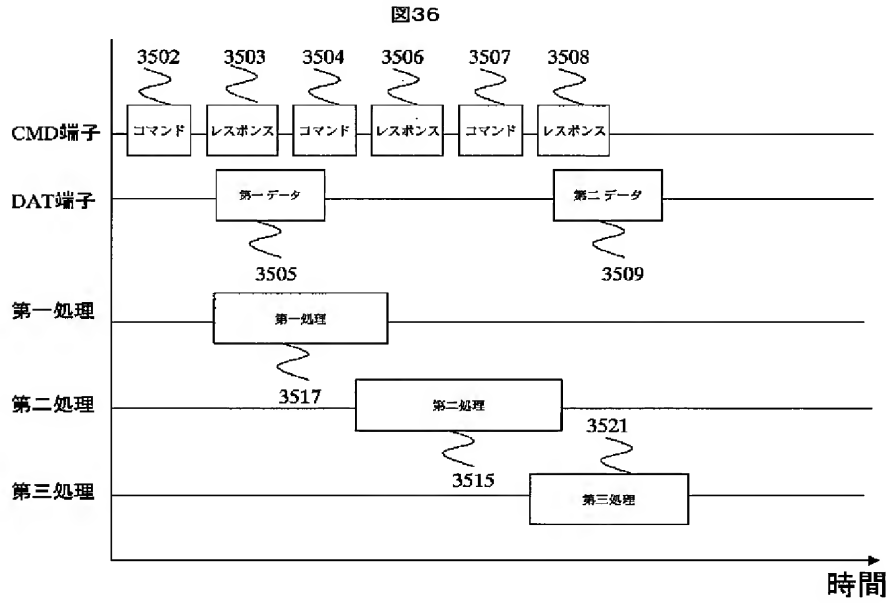
【図３５】

図35



【図３６】

図36



フロントページの続き

(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　片山　国弘
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

Ｆターム(参考)　2C005 MA19 MB02 MB07 NA10 PA18
PA21 RA22 WA03 WA09
5B017 AA07 BA06 BA07 CA14
5B035 AA13 BB09 BC00 CA07 CA11
CA29